

AWARD/CONTRACT		1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		RATING		PAGE OF PAGES 1 83	
2. CONTRACT (Proc. Inst. Ident.) NO. N66001-16-D-0205		3. EFFECTIVE DATE 11 Jul 2016		4. REQUISITION/PURCHASE REQUEST/PROJECT NO. 1300339415			
5. ISSUED BY SPAWAR SYSTEMS CENTER PACIFIC MATT SCHUPBACH, CODE 22550 MATTHEW.SCHUPBACH@NAVY.MIL 53560 HULL STREET SAN DIEGO CA 92152		CODE N66001	6. ADMINISTERED BY (If other than Item 5) DCMA ATLANTA 2300 LAKE PARK DRIVE SUITE 300 SMYRNA GA 30080-4091		CODE S1103A		SCD: C
7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, county, state and zip code) SCIENTIFIC RESEARCH CORPORATION DUNS#: 197138274 2300 WINDY RGE PWY STE 400S ATLANTA GA 30339-8431				8. DELIVERY [] FOB ORIGIN [X] OTHER (See below)			
				9. DISCOUNT FOR PROMPT PAYMENT			
				10. SUBMIT INVOICES 1 (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN:		ITEM Section G	
CODE 0D5A6		FACILITY CODE					
11. SHIP TO/MARK FOR See Schedule		CODE	12. PAYMENT WILL BE MADE BY DFAS COLUMBUS CENTER DFAS-CO/SOUTH ENTITLEMENT OPERATIONS P.O. BOX 182264 COLUMBUS OH 43218-2264		CODE HQ0338		
13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: [] 10 U.S.C. 2304(c)() [] 41 U.S.C. 253(c)()		14. ACCOUNTING AND APPROPRIATION DATA					
15A. ITEM NO.	15B. SUPPLIES/ SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT		
SEE SCHEDULE							
15G. TOTAL AMOUNT OF CONTRACT							\$20,436,260.38
16. TABLE OF CONTENTS							
(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/ CONTRACT FORM	1	X	I	CONTRACT CLAUSES	52 - 82
X	B	SUPPLIES OR SERVICES AND PRICES/ COSTS	2 - 6	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/ SPECS./ WORK STATEMENT	7 - 28	X	J	LIST OF ATTACHMENTS	83
X	D	PACKAGING AND MARKING	29	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE	30	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS		
X	F	DELIVERIES OR PERFORMANCE	31				
X	G	CONTRACT ADMINISTRATION DATA	32 - 36	L	INSTRS., CONDS., AND NOTICES TO OFFERORS		
X	H	SPECIAL CONTRACT REQUIREMENTS	37 - 51	M	EVALUATION FACTORS FOR AWARD		
CONTRACTING OFFICER WILL COMPLETE ITEM 17 (SEALED-BID OR NEGOTIATED PROCUREMENT) OR 18 (SEALED-BID PROCUREMENT) AS APPLICABLE							
17. [X] CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 1 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)				18. [] SEALED-BID AWARD (Contractor is not required to sign this document.) Your bid on Solicitation Number N66001-15-R-0037-0002 including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the terms listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)			
19A. NAME AND TITLE OF SIGNER (Type or print)				20A. NAME OF CONTRACTING OFFICER STACIE SEDGWICK / SUPERVISOR TEL: 619-553-5587 EMAIL: stacie.sedgwick@navy.mil			
19B. NAME OF CONTRACTOR BY _____ (Signature of person authorized to sign)		19C. DATE SIGNED		20B. UNITED STATES OF AMERICA BY _____ (b)(6) (Signature of Contracting Officer)		20C. DATE SIGNED 07-Jul-2016	

AWARD/CONTRACT		1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		RATING		PAGE OF PAGES 1 83	
2. CONTRACT (Proc. Inst. Ident.) NO. N66001-16-D-0205		3. EFFECTIVE DATE 7/11/2016		4. REQUISITION/PURCHASE REQUEST/PROJECT NO. 1300339415			
5. ISSUED BY SPAWAR SYSTEMS CENTER PACIFIC MATT SCHUPBACH, CODE 22550 MATTHEWSCHUPBACH@NAVY.MIL 63560 HULL STREET SAN DIEGO CA 92162		CODE N66001		6. ADMINISTERED BY (If other than Item 5) DCMA ATLANTA 2300 LAKE PARK DRIVE SUITE 300 SMYRNA GA 30080-4091		CODE S1103A SCD: C	
7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, county, state and zip code) SCIENTIFIC RESEARCH CORPORATION DUNSH: 197138274 2300 WINDY RGE PWY STE 400S ATLANTA GA 30339-8431				8. DELIVERY [] FOB ORIGIN [X] OTHER (See below)			
				9. DISCOUNT FOR PROMPT PAYMENT			
CODE 0D5A6				FACILITY CODE		10. SUBMIT INVOICES 1 (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN: ITEM Section G	
11. SHIP TO/MARK FOR See Schedule		CODE		12. PAYMENT WILL BE MADE BY DFAS COLUMBUS CENTER DFAS-CO/SOUTH ENTITLEMENT OPERATIONS P.O. BOX 182264 COLUMBUS OH 43218-2264		CODE HQ0338	
13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: [] 10 U.S.C. 2304(c)() [] 41 U.S.C. 253(c)()				14. ACCOUNTING AND APPROPRIATION DATA			
15A. ITEM NO.	15B. SUPPLIES/ SERVICES		15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT	
SEE SCHEDULE							
15G. TOTAL AMOUNT OF CONTRACT						\$20,436,260.38	
16. TABLE OF CONTENTS							
(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/ CONTRACT FORM	1	X	I	CONTRACT CLAUSES	52 - 82
X	B	SUPPLIES OR SERVICES AND PRICES/ COSTS	2 - 6	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/ SPECS/ WORK STATEMENT	7 - 28	X	J	LIST OF ATTACHMENTS	83
X	D	PACKAGING AND MARKING	29	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
X	E	INSPECTION AND ACCEPTANCE	30	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS		
X	F	DELIVERIES OR PERFORMANCE	31				
X	G	CONTRACT ADMINISTRATION DATA	32 - 36	L	INSTRS., CONDS., AND NOTICES TO OFFERORS		
X	H	SPECIAL CONTRACT REQUIREMENTS	37 - 51	M	EVALUATION FACTORS FOR AWARD		
CONTRACTING OFFICER WILL COMPLETE ITEM 17 (SEALED-BID OR NEGOTIATED PROCUREMENT) OR 18 (SEALED-BID PROCUREMENT) AS APPLICABLE							
17. [X] CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 1 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)				18. [] SEALED-BID AWARD (Contractor is not required to sign this document.) Your bid on Solicitation Number N66001-15-R-0037-0002			
19A. NAME AND TITLE OF SIGNER (Type or print) Frank McKenna, Contract Administrator				20A. NAME OF CONTRACTING OFFICER Stacie L. Sedgwick TEL: 619-553-5587 EMAIL: stacie.sedgwick@navy.mil			
19B. NAME OF CONTRACTOR BY <i>Frank McKenna</i> (Signature of person authorized to sign)		19C. DATE SIGNED 7 July 2016		20B. UNITED STATES OF AMERICA BY <i>[Redacted]</i> (b)(6) (Signature of Contracting Officer)		20C. DATE SIGNED 7 Jul 16	

Section B - Supplies or Services and Prices

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Services IAW PWS CPFF Engineering and Technical Services IAW the Performance Work Statement (PWS) (See Section C). Base Period (3 Years). FOB: Destination PURCHASE REQUEST NUMBER: 1300339415		Lot		\$20,436,260.38
				ESTIMATED COST	(b)(4)
				FIXED FEE	(b)(4)
				TOTAL EST COST + FEE	\$20,436,260.38

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Contract Data Requirements - NSP		Lot		NSP

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001 OPTION	Services IAW PWS - OYI CPFF Engineering and Technical Services IAW the Performance Work Statement (PWS) (See Section C). Option Year I FOB: Destination		Lot		(b)(4)
				ESTIMATED COST	(b)(4)
				FIXED FEE	(b)(4)
				TOTAL EST COST + FEE	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002			Lot		NSP
OPTION	Contract Data Requirements OYI - NSP				

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001			Lot		(b)(4)
OPTION	Services IAW PWS OYII CPFF Engineering and Technical Services IAW the Performance Work Statement (PWS) (See Section C). Option Year II FOB: Destination				
				ESTIMATED COST	(b)(4)
				FIXED FEE	(b)(4)
				TOTAL EST COST + FEE	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002			Lot		NSP
OPTION	Contract Data Requirements OYII - NSP				

CLAUSES INCORPORATED BY FULL TEXT

5252.216-9200 PAYMENT OF FIXED FEE (COMPLETION TYPE) (JAN 1989)

FIXED FEE: See Maximum Base Period Fee on CLIN 0001 and Maximum Option Period Fee on CLINs 1001 and 2001. Fee amounts will be specified on individual task orders. The Government shall make payment to the Contractor when requested as work progresses, but no more frequently than biweekly, on account of the fixed fee, equal to a maximum of (b)(4) on prime labor, (b)(4) on subcontract labor, and (b)(4) on Other Direct Cost amounts

invoiced by the Contractor under the "Allowable Cost and Payment" clause hereof for the related period, subject to the withholding provisions of paragraph (b) of the "Fixed Fee" clause. In the event of discontinuance of the work in accordance with clause of this contract entitled "Limitation of Cost" the fixed fee shall be redetermined by mutual agreement equitably to reflect the diminution of the work performed; the amount by which such fixed fee is less than, or exceeds payments previously made on account of fee, shall be paid, or repaid by, the Contractor, as the case may be.

(End of clause)

5252.216-9204 LEVEL OF EFFORT--FEE ADJUSTMENT FORMULA (MAR 1994)

(a) Subject to the provisions of the "Limitation of Cost" or "Limitation of Funds" clause (whichever is applicable to this contract), it is hereby understood and agreed that the fixed fee is based upon the Contractor providing the below listed number of staff-hours of direct labor, hereinafter referred to as X, at the estimated cost and during the term of this contract specified elsewhere herein:

CLIN

Total Staff-hours
of Direct Labor (X)

*

*

* CLIN and number of labor hours will be determined on level-of-effort task orders and will be specified in a DD Form 1155. Contractor fee shall not exceed the amounts proposed for the basic contract (a maximum of (b)(4) on prime labor, (b)(4) on subcontract labor, and (b)(4) on Other Direct Cost amounts).

The Contractor agrees to provide the total level of effort specified above in performance of work described in Sections "B" and "C" of this contract. The total staff-hours of direct labor shall include subcontractor direct labor hours for those subcontractors identified in the Contractor's proposal as having hours included in the proposed level of effort.

(b) Of the total staff-hours of direct labor set forth above, it is estimated that 0 staff-hours are competitive time (uncompensated overtime). Competitive time (uncompensated overtime) is defined as hours provided by personnel in excess of 40 hours per week without additional compensation for such excess work. All other effort is defined as compensated effort. If no amount is indicated in the first sentence of this paragraph, competitive time (uncompensated overtime) effort performed by the contractor shall not be counted in fulfillment of the level of effort obligations under this contract.

(c) Effort performed in fulfilling the total level of effort obligations specified above shall only include effort performed in direct support of this contract and shall not include time and effort expended on such things as local travel from an employee's residence to their usual work location, uncompensated effort while on travel status, truncated lunch periods, or other time and effort which does not have a specific and direct contribution to the tasks described in Section B.

(d) It is understood and agreed that various conditions may exist prior to or upon expiration of the term of the contract, with regard to the expenditure of labor staff-hours and/or costs thereunder which may require adjustment to the aggregate fixed fee. The following actions shall be dictated by the existence of said conditions:

(1) If the Contractor has provided not more than 105 % of X or not less than 95 % of X, within the estimated cost, and at the term of the contract, then the fee shall remain as set forth in Section B.

(2) If the Contractor has provided X-staff-hours, within the term, and has not exceeded the estimated cost then the Contracting Officer may require the Contractor to continue performance until the expiration of the term, or until the expenditure of the estimated cost of the contract except that, in the case of any items or tasks funded with

O&MN funds, performance shall not extend beyond 30 September. In no event shall the Contractor be required to provide more than 105 % of X within the term and estimated cost of this contract. The fee shall remain as set forth in Section B.

(3) If the Contractor expends the estimated cost of the contract, during the term of the contract and has provided less than X staff-hours, the Government may require the Contractor to continue performance, by providing cost growth funding, without adjusting the fixed fee, until such time as the Contractor has provided X staff-hours.

(4) If the Contracting Officer does not elect to exercise the Government's rights as set forth in paragraph (d)(2) and (d)(3) above, and the Contractor has not expended more than 95 % of X staff-hours, the fixed fee shall be equitably adjusted downward to reflect the diminution of work.

(5) Nothing herein contained shall, in any way, abrogate the Contractor's responsibilities, and/or the Government's rights within the terms of the contract provision entitled "Limitation of Cost" or "Limitation of Funds" as they shall apply throughout the term of the contract, based upon the total amount of funding allotted to the contract during its specified term.

(e) Within 45 days after completion of the work under each separately identified period of performance hereunder, the Contractor shall submit the following information in writing to the Contracting Officer with copies to the cognizant Contract Administration Office and DCAA office to which vouchers are submitted:

(1) The total number of staff-hours of direct labor expended during the applicable period.

(2) A breakdown of this total showing the number of staff-hours expended in each direct labor classification and associated direct and indirect costs.

(3) A breakdown of other costs incurred.

(4) The Contractor's estimate of the total allowable cost incurred under the contract for the period.

In the case of a cost under-run, the Contractor shall submit the following information in addition to that required above:

(5) The amount by which the estimated cost of this contract may be reduced to recover excess funds and the total amount of staff-hours not expended, if any.

(6) A calculation of the appropriate fee reduction in accordance with this clause.

All submissions required by this paragraph shall include subcontractor information, if any.

(f) SPECIAL INSTRUCTION TO THE PAYING OFFICE REGARDING WITHHELD FEE

Fees withheld pursuant to the provisions of this contract, such as the withholding provided by the "Allowable Cost and Payment" and "Fixed Fee" clauses, shall not be paid until the contract has been modified to reduce the fixed fee in accordance with paragraph (d) above, except that no such action is required if the total level of effort provided falls within the limits established in paragraph (d) above.

(End of clause)

5252.216-9218 MINIMUM AND MAXIMUM QUANTITIES (JUL 1989)

As referred to in paragraph (b) of the "Indefinite Quantity" clause of this contract, the contract minimum quantity is a total of \$6,667.00 worth of orders for each contract at the contract unit price(s). The maximum quantity is the total estimated amount of the contract. The maximum quantity is not to be exceeded without prior approval of the Procuring Contracting Officer.

The combined/overall ceiling for all awards under this Multiple Award Contract is \$49,820,186.97; however, no MAC awardee can exceed the value of its contract maximum quantity specified in Section B.

(End of clause)

5252.232-9210 LIMITATION OF LIABILITY--INCREMENTAL FUNDING (JAN 1992)

This task order (when specified in the task order) is incrementally funded and the amount currently available for payment hereunder is limited to \$ * inclusive of fee. It is estimated that these funds will cover the cost of performance through *. Subject to the provisions of the FAR 52.232-22 "Limitation of Funds" clause of this contract, no legal liability on the part of the Government for payment in excess of \$ * shall arise unless additional funds are made available and are incorporated as modifications to this contract.

*To be specified in incrementally funded Task Orders.

(End of clause)

Section C - Descriptions and Specifications

SPECIFICATIONS**Performance Work Statement**

For

Engineering and Support Services for Network and Information Systems Technology Programs
04 November 2015

1.0 SCOPE

The Networks Division (Code 55100) at Space and Naval Warfare Systems Center, Pacific (SSC Pacific) has identified requirements for engineering and technical services in support of networks, communication systems, sensors, applications and information systems that are currently operational, under development, requiring upgrades or theoretical. The networks and systems described and referred to in this Performance Work Statement (PWS) are specialized afloat, ashore and airborne networks that enable net-centric operations including Command and Control (C2) in naval, joint, allied or coalition operations. SSC Pacific Code 55100 develops and validates Concept of Operations (CONOPS), Tactics Techniques and Procedures (TTP), protocols, security posture, and architectures on networks which operate both within the overall United States exclusive military/government domain with extension into the public realm, and leverages commercial networks and information assets. More importantly, networks provide the gateway to achieving information dominance in the cyberspace domain, and for Net-centric operations achieving warfighter superiority.

SSC Pacific Code 55100 provides for continuing Command, Control, Communications, Computer and Intelligence Surveillance Reconnaissance (C4ISR) systems engineering support related to the core competencies of technology and architecture development, network analysis, modeling, and simulation, network convergence, network timing, network security, certification and governance, network and information system applications, network management and monitoring, network and computer operations, and production and manufacturing processes. SSC Pacific Code 55100 also engineers the network interfaces and interconnections with Radio Frequency (RF) communication systems both tactical and beyond line of sight, and connectivity with RF terminals, sensors, and end-user applications and data storage/processing centers.

SSC Pacific Code 55100 plans, establishes and manages network and information systems for Programs of Record (PoR) and projects in support of Department of Defense (DoD) requirements, as well as associated composite programs. This begins at the concept formulation stages and extends through experimentation, system validation, fleet installation and operational support. It includes performing systems engineering, project analysis, hardware and software design, system design and integration, test and evaluation, and technical management throughout the scope of the program or project. In addition, systems engineering practices include reliability, maintainability, supportability and affordability analysis and implementation.

SSC Pacific Code 55100 engages in activities from basic research of Science and Technology (S&T) through Research and Development (R&D), to production, integration, deployment and operational support producing superior and scalable architectures and systems. Acting as the Technical Authority (TA) for networks, SSC Pacific Code 55100 provides technical leadership, technical expertise and consultation to the acquisition and Research Development Test & Evaluation (RDT&E) communities, military offices, commands and operational forces. In addition, applying Capability Maturity Model Integration (CMMI), Project Management Guide (PMG), and industry best practices, these process improvement approaches position SSC Pacific Code 55100 with the essential elements to continue improvement and optimization, identify organizational processes' strengths and weaknesses, increase performance and generate the highest quality solutions and products.

The following Commands, Agencies, Programs, Projects, Activities and Areas of Investigation are supported within SSC Pacific Code 55100:

AEGIS Ashore

Airborne Networking

Anti-Access/Area Denial (A2/AD)

Applications Integration (AI)

Automated Digital Network System (ADNS)

Ballistic Missile Defense (BMD)

Ballistic Missile Defense (BMD) Multi-cast TADIL-J (MTJ)

Base Level Information Infrastructure Piers (BLII PIERS)

Battle Force Tactical Network (BFTN)
Broad Area Maritime Surveillance (BAMS) and Multi-mission Maritime (MMA) Aircraft
Cloud Computing Strategy
Coalition Information Exchange System
Coastal Surveillance System Network (CSSN)
Combatant Commanders (COCOM HQ)
Combined Enterprise Regional Information Exchange System (CENTRIX)
Commanders Secure Network (CSN)
Commercial Broadband Satellite Program (CBSP)
Common Data Link (CDL) Including: CDL-S, Tactical CDL, NT-CDL variants
Consolidated Afloat Networks and Enterprise Services (CANES)
Cryptologic Carry On Program (CCOP)
Cyber Test Analysis and Simulation Environment (TASE)
Cyber Situational Awareness (Cyber SA)
Data Center Consolidation (DCC)
Defense Advanced Research Projects Agency (DARPA)
Defense Information Systems Agency (DISA)
Defense Red Switch Network (DRSN)
Deployable Joint Command & Control (DJC2)
Directional Adhoc Networking Technology (DANTE)
Distributed Common Ground System (DCGS)
Energy Harvesting
Foreign Military Sales (FMS)
Full Motion Video (FMV)
Global Information Grid (GIG)
Gigabit Passive Optical Networks (GPON)
High Assurance Internet Protocol Encryptor (HAIZE)
High Performance Computing (HPC)
Hostile-forces Targeting Service (HITS)
Information Assurance (IA)
Integrated Shipboard Network System (ISNS)
Internet Protocol Version 6 (IPv6) Transition
IT Infrastructure & Operational Efficiencies
Joint Aerial Layer Network (JALN)
Joint Capability Technology Demonstration (JCTD)
Joint Communications Simulation System (JCSS)
Joint Information Environment (JIE)
Joint Network-Centric Operations (JNO)
Joint Tactical Networking Center (JTNC)
Maritime Domain Awareness (MDA)
Maritime Operation Center (MOC)
Military Satellite Communications (MILSATCOM)
Mobile User Objective System (MUOS)
Model Verification and Validation
National Geospatial-Intelligence Agency (NGA)
National Reconnaissance Office (NRO)
National Security Agency (NSA)
Naval Air Systems Command (NAVAIR)
Naval Computer and Telecommunications Area Master Stations (NCTAMS)
Naval NETWAR FORCEnet Enterprise (NNFE)
Naval Sea Systems Command (NAVSEA)
Navy Air Operations Command & Control (NAOC2)
Navy and Marine Corp Manned Air Vehicles (i.e. EA-6B, E-2C/D, EP-3E, H-60, P-3C, P-8A, F-35, H-53, V-22 etc.)
Navy Ballistic Missile Defense Enterprise (NBMDE)

Navy Networking Environment 2016 (NNE 16)
 Navy Task Force Enterprise Computing Environment (TF CLOUD)
 Network Convergence
 Network on the Move (NOTM)
 Next Generation Enterprise Network (NGEN)
 OPNAV N81 Assessments
 OPNET Modeling and Simulation
 QualNet Modeling and Simulation
 Signal Characterization and Emitter Identification
 Risk Management Framework
 RF Communications (HF, VHF, UHF, SHF, EHF, AEHF etc.)
 Satellite Communications (Commercial and Military)
 Satellite Tool Kit (STK) Modeling and Simulation
 Sensitive Compartmented Intelligence (SCI) Networks PoR
 SPAWAR System Command
 SUBLAN
 Sub Net Rely (SNR)
 Tactical Data Links (TDL)
 Tactical Switching (TSw)
 Tactical Operation Center (TOC)
 Target Technical Framework (TTF)
 Task Force Web
 Teleport Earth Ground Stations
 Theater Net-Centric Geolocation (TNG)
 Unmanned Carrier Launched Airborne Surveillance and Strike Systems (UCLASS)
 Unmanned Systems (Ground, Sea, Air variants)
 USAF, US Army and VIP Aircraft
 Voice over IP (VoIP)
 Voice Video over Secure Internet Protocol (VVoSIP)
 WAN Optimization
 Wireless Mobile Networking

2.0 APPLICABLE DOCUMENTS

Applicable documents will be added at the task order level and may include military standards, military handbooks, software development guidance, and other publications.

3.0 TECHNICAL REQUIREMENTS

Under SSC Pacific Transport and Computing Infrastructure (TCI) Portfolio construct, SSC Pacific Code 55100 anticipates work that will include the Ashore, Afloat, Subsurface, Airborne, Mobile, Joint, and Federal Infrastructure business areas with specific technologies such as network design and development, network monitoring, management and operations, common computing environment, infrastructure with associated hardware and software components, cloud computing, ashore and afloat data centers and server hosting environments, consolidated network enterprise services, wireless networking, and tactical, satellite and joint space communications. Transformation of capabilities-based portfolio into a networked infrastructure enables Information Dominance through Navy and Joint net-centric operations.

Aligned with Program Executive Office (PEO) C4I Master Plan, three tenets guide the transition to a net-centric infrastructure:

Mission-centered (Mission): The TCI portfolio of systems is evolving to support the Navy's focus on cross-functional mission execution in accordance with Naval Operation Concept for Joint Operations and the Chief of Naval Operations (CNO) Information Dominance Vision. Careful consideration is being given to approved and evolving mission threads in order to validate the relevance of the portfolio over time. Key operational threads include: Anti-Submarine Warfare (ASW), Ballistic Missile Defense (BMD), Close Air Support (CAS), Commander Joint Task Force (CJTF), Intelligence, Surveillance and Reconnaissance (ISR): Tasking, Collection, Processing,

Exploitation, Dissemination (TCPED), Joint Force Maritime Component Commander (JFMCC), Maritime Domain Awareness (MDA), Maritime Interdiction (MI)/Anti-Surface Warfare (ASuW), Navy Networking Environment (NNE), and Anti-Access Area Denial (A2AD). The end objective is to deliver capabilities and services that are available upon demand and integrated in the context of the mission(s) to be executed, with the infrastructure supporting all mission applications being nearly transparent to the war fighter.

Standards-compliant (Technical): The transition is based on a standards-based open architecture that shall readily adapt to the incorporation of future technologies, shall facilitate the retirement of legacy capabilities, and shall reduce the facilities required to house legacy capabilities, resulting in significant savings in the long term. Furthermore, adherence to standards contained within the DoD Information Technology Standards Repository (DISR) (<https://disronline.disa.mil>) and the Net-Centric Enterprise Solutions for Interoperability (NESI) (<http://nesipublic.spawar.navy.mil>) shall enable the development of interoperable net-centric capabilities. Ongoing standards collaboration with the Intelligence Community (IC) is critical to promoting data interoperability between DoD and IC systems through the implementation of shared cloud architectures and associated standards. Finally, commercial standards and best practices, such as those being developed by American National Standard Institute (ANSI) under the Network Centric Operations Industry Consortium (<http://www.ncoic.org/>), shall be leveraged to guide the technical implementation of DoD's net-centric and data-centric capabilities.

Directives-compliant (Programmatic): In order to deliver networked systems that are compliant with the latest policies, guidance and direction, focus of efforts shall leverage the following documentations:

- a) Global Information Grid Architecture v2.0,
- b) DoD Net-Centric Data Strategy,
- c) DoD Architectural Framework v2.0,
- d) DODI 5000.02, CJCSI 3170.01H which is the new update to the Joint Capabilities Integration and Development System (JCIDS) instruction,
- e) CJCSI 6212.01E which prescribes Net-Ready Key Performance Parameter (NR-KPP) compliance
- f) Other technical directives and initiatives from DoD and DoN.

Systems Engineering for Networks and Communications: Systems engineering comprises the full scope of work from solution analysis, technology development, engineering and manufacturing development, production and deployment, operations and support across the complete end-to-end system and across the complete life cycle, in support of projects and programs for ships, submarines, aircraft, unmanned systems and shore facilities.

Solutions Analysis: The objective of Solution Analysis is to select and adequately describe a preferred materiel solution to satisfy the requirements of the stakeholders. A high level system model/architecture and preliminary system performance specification are developed, and establishes a basis for Technology Development.

Technology Development: The objective of Technology Development is to reduce technical risk and develop a sufficient understanding of the materiel solution to support sound decisions leading into Engineering and Manufacturing Development. This includes maturing technology, prototyping system elements, and refining requirements, specifications, interfaces and system model/architectures.

Engineering and Manufacturing Development: The objective of Engineering and Manufacturing Development is to develop the detailed product baseline, verify it meets the system functional requirements, transform the preliminary design into a producible design, assess risk levels for the system, and prepare for production or deployment.

Production and Deployment: The objective of Production and Deployment is to validate the product design and to deliver the quantity of systems required for full operating capability, including all enabling system elements and supporting material and services. Deliver the final product baseline as validated during operational testing, and supports deployment and transition of capability to all end users, the warfighters, and supporting organizations. The maintenance approach, training, and technical manuals, should be integrated with Production and Development along with specific test and evaluation and logistics and sustainment activities.

Operations and Support: The objective of Operations and Support is to execute a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle.

The following requirements comprise the scope of Systems Engineering efforts anticipated to support SSC Pacific Code 55100 work related to networks and communications to enable net-centric capabilities of controllers, sensors, processors, monitoring and management components, platforms and installations across enterprise domains.

3.1 Systems Engineering: Capabilities, Requirements, and Assessments

3.1.1 Capabilities, Requirements and Assessments

The contractor shall analyze the capabilities and environmental constraints identified from users, sponsors or stakeholders of network and communication systems, and generate performance and functional requirements to realize those capabilities. The solution may be for a new project or upgrade to an existing system. The contractor must be able to decompose high level requirements into functional definitions, verification objectives, and full system specifications, identifying enabling and critical technologies, constraints and risks. The contractor shall assess and analyze system concepts, functional capabilities, and performance specifications and validate against user needs. Assessments would include system specifications, safety considerations, maintenance concepts, cost and manpower estimates, testing and support strategies, and feasibility studies of the impacts of integrating new capabilities or technology into existing or currently fielded systems.

3.1.2 Science & Technology

The contractor shall be able to support Science and Technology (S&T) research and generate concepts, designs and models the will realize future objectives and requirements. Research will push state-of-the-art capabilities enabling advances that will yield superiority for the warfighter, especially in the area of Information Dominance.

3.2 Systems Engineering: Architecture Research and Design

A detailed architecture design establishes the initial building blocks and framework for a project demonstration or a system deployment, and must address all interfaces and interactions internal and external to the system.

3.2.1 Enterprise Level

The contractor shall develop enterprise level architectures that address and are consistent with DoD rules and policies to provide frameworks for data, application, technology and business strategies and that are technically feasible and responsive to changing mission needs. The contractor shall mature technology to higher level readiness levels. The contractor shall produce DoD Architecture Framework (DoDAF) documents showing integrated architectures across multiple views.

3.2.2 Tactical Level

The contractor shall develop architectures that extend to the tactical level that may transverse the GIG which shows interfaces and connectivity between shore terrestrial locations and forward deployed nodes either stationary or mobile. This would include components, interfaces, software to achieve system requirements and insure compatibility across the DoD enterprise, and with other tactical users.

3.2.3 System Level

The contractor shall design systems for reliability, maintainability, and supportability, and that reduce the overall program risk from the viewpoint of cost, schedule and performance. The contractor shall provide redesign plans for improvements to capabilities of next generation systems.

3.3 Systems Engineering: Modeling and Simulation

The intent of this section is to provide engineering and development services for conducting analysis of Joint and Naval C4ISR architectures and capabilities utilizing Modeling and Simulation.

3.3.1 Types of Models Utilized

The contractor shall provide engineering and development support of rigorous technical assessments utilizing a variety of different tools in order to analyze the full spectrum of C4ISR. This specifically includes, but is not limited to, the following types of models and tools:

- Network Performance Assessment Models
- System and Network-level Cyber Attack and Defense Models
- RF Propagation and Antennae Modeling
- Satellite Communications (SATCOM) Modeling
- Mathematic Algorithm Modeling
- Mission (Force-on-Force) Modeling
- Process Modeling

Providing of engineering services to develop or enhance simulation tools will be required if the requisite capabilities do not exist in a readily available commercial or government simulation tool.

Modeling and Simulation will occur on multiple security levels up to and including TS/SCI.

3.3.1.1 Network Performance Assessment Models:

Provide engineering and development services in the construction and integration of network and protocol models using Joint Communications Simulation System (JCSS) (GOTS), Operational Network (OPNET), QualNet or equivalent simulator high-performance engineering level network modeling environment.

3.3.1.2 System and Network-level Cyber Attack and Defense Models:

Provide engineering and development services in the construction and integration of network Cyber models using Exata Cyber modeling environment or equivalent simulator. This shall include the development of tools capable of analyzing the impact of Cyber threats on the C4ISR system being assessed.

3.3.1.3 RF Propagation and Antennae Modeling (i.e. Interactive Scenario Builder):

Provide engineering and development services in the construction and integration of RF Propagation and Antennae models using OPNET, Systems Tool Kit (STK), Interactive Scenario Building (GOTS), SPEED (GOTS), or equivalent RF/Antennae simulator.

3.3.1.4 Satellite Communications Modeling:

Provide engineering and development services in the construction and integration of satellite models for conducting communication performance assessments using OPNET, STK, or equivalent SATCOM model. SATCOM models will be used to determine mechanisms for achieving greater efficiency, predicting performance of current and future systems, and conducting end-to-end analysis. SATCOM models may require development at down to the Media Access Control (MAC) and Physical Layers.

3.3.1.5 Mathematic Algorithm Modeling:

Provide engineering and development services in the construction and integration of mathematical models using MATLAB or other equivalent simulator. Mathematical models are used for a variety of different applications, such as development of more efficient protocols and algorithms and models of mathematically intense physic environments not capable of being modeled with other explicit simulation environments today.

3.3.1.6 Mission (Force-on-Force) Modeling:

Provide engineering and development services in the construction and integration of mission models using Naval Simulation Systems (NSS) or other equivalent simulator. Mission models are used to assess the impact that different C4ISR capabilities have on the Navy's ability to effectively fight wars and tackle various small operational scenarios.

3.3.1.7 Process Modeling:

Provide engineering and development services in the construction and integration of process models using Extend, Provision, or equivalent process model simulator. Assessments shall be used to assess product development cycles and workflows.

3.3.2 Execution of Analysis

The contractor shall provide engineering and developmental services across the Modeling and Simulation Analysis Process. The process followed by SSC Pacific, Code 551 is as follows:

- Gather Requirements and Scope Study
- Design the Experiment
- Conduct Data Collection
- Build Out Simulation Models
- Execute Simulations
- Analyze Results and Execute Updates or Excursions
- Document and Present Data Collected and Utilized, Model Configurations, Assumptions, Results, and Findings to Management and Stakeholders
- Promote Model Reuse and Interoperability

Specific requirements for each of these areas are documented in the following sub-sections.

3.3.2.1 Gather Requirements and Scope Study:

Extract key deliverables, critical technologies, available models and modeling tools, important takeaways, and available data and resources and utilize formulate the requirements of the assessment and utilize to scope the assessment.

3.3.2.2 Design the Experiments:

Based upon the assessment's requirements and scope; determine the required data, appropriate tool and level of fidelity for executing the assessment, computational requirements for conducting the assessment, number of simulation runs required to achieve statistical significance (if stochastic processes or random number generators are utilized in the model), and begin to identify Measures of Performance (MoPs) and Measures of Effectiveness (MoEs) that will be relevant for the experiment.

3.3.2.3 Conduct Data Collection:

Conduct the required data collection exercises necessary to build accurate, reproducible C4ISR models. These activities shall include but are not limited to:

- Collaboration with other teams, modelers, engineers, program managers, or Subject Matter Experts (SMEs) to collect required technical information, interfaces, specifications, requirements to be able to accurately represent the technical aspects of the subject material.
- Perform engineering analysis, development, and documentation of Navy and Joint Information Exchange Requirements (IERs) for use in M&S activities.
- Perform data collection on systems and applications (either Afloat or Ashore) corresponding to information exchange requirements.
- Perform data collection on systems and applications to derive traffic profiles for constructive simulations.
- Collect data on representative Cyber threats and system vulnerabilities.

3.3.2.4 Build Out Models for Simulations:

Provide engineering and development services in the construction and integration of simulation models in the appropriate tool utilizing the data available. Depending upon the scope of problems being assessed, several models in different tools may be required to fully cover the scope of the requirements. If several models are required, then results shall be feed from one model to the next either in an online or offline manner.

Provide engineering and development services with the requisite knowledge base in modeling and simulation, stochastic processes and queuing theory, the appropriate tools utilized for the assessment, and in the critical technologies being assessed.

3.3.2.5 Execute Simulations:

Provide engineering and development services for executing the simulation or series of simulations. If updates are determined during the analysis or execution phase, make required updates to the models and re-perform the execution of the simulations.

3.3.2.6 Analyze Results and Execute Updates or Excursions:

Provide engineering and analysis services for extraction simulation results out of the simulator, processes the data using common office tools such as Microsoft Excel (or equivalent) to writing custom Perl or Java Scripts to parse through data. Understand how probability, statistics, and stochastic processes may impact results and tie results together from a series of simulation runs.

Provide engineering and development services for creating plots, tables, and summaries of data collected and determine key findings. Assess and understand the results and their applicability to systems under assessment to determine validity and credibility of results. Determine if updates to the models are required. Roll technical data or performance parameters up into Measures of Effectiveness.

3.3.2.7 Verification and Validation of Models:

Provide engineering and development services for verifying that the simulation models accurately represent the technological elements. Ensure that any code developed accurately depicts the system characteristics that it is trying to represent, that all parameters were properly configured, and that statistics received align with any available real world data.

Provide engineering and development services for validating that the simulation models accurately demonstrated the operational relevance of the C4ISR system. The contractor shall work with the operational community to understand the systems operational requirements.

Verification and validation efforts may be conducted for models performed by SSC Pacific under this task order or may be for independent assessments conducted for other Government entities.

3.3.2.8 Document and Present Findings to Management and Stakeholders:

Provide engineering and analysis services to document the data collected and utilized during the modeling efforts, the precise model configurations and excursions, assumptions used in developing the models and concept of operations, the results and findings.

Provide reports and both technical and executive level briefings to the management and stakeholders of the assessment.

3.3.2.9 Promote Model Reuse and Interoperability:

Provide engineering services that understand relevant other efforts ongoing within their organization and Government organization that can promote reuse of code, models, and data collected.

Provide engineering and development services that work on model interoperability to federate data and results between models.

3.4 Systems Engineering: Engineering Development

3.4.1 Network and Communication Development

The contractor shall develop, build and integrate the components and sub-systems required to realize capability requirements and/or designed system architectures. The contractor shall develop software and applications required to realize designed system functionality and capability. The contractor shall develop, build and integrate networking and processing capabilities in virtualized environments utilizing emerging technologies.

3.4.2 Integration with Communication Systems

The contractor shall perform systems engineering and technical analyses to support the integration of communications connectivity via commercial or military Satellite Communications (SATCOM) systems, and direct Line of Sight (LOS) communication systems with existing and future networks. The engineering development extends to multi-band commercial systems, components, antennas including low observable multi-function antenna systems, and electromagnetic interference evaluation of platforms and facilities to ensure electromagnetic compatibility.

3.4.3 Improvements and Technical Evaluations

Based on technical evaluations and reviews the contractor shall re-design sub-systems or systems for better functionality, reliability and sustainability that mitigate risk in planned operations.

3.4.4 Use of Prototypes

The contractor shall use prototypes to mature system designs and drawings, and to evaluate selected technology for future production or manufacturing.

The contractor shall build or fabricate assemblies and systems including Engineering Development Models (EDM) when needed and which align with system acquisition strategy.

Then contractor shall design/redesign Circuit Card Assembly (CCA), assemble limited production Printed Wiring Boards (PWBs), and install and test components or subsystems in analog, digital or hybrid systems employing general technician support or expertise.

3.4.5 Engineering Documentation and Reviews

The contractor shall perform documentation and distribution of engineering and computer related information. The contractor shall develop block diagrams, technical sequences, flow charts, work breakdown structures. The contractor shall develop, modify, and/or update specifications; Computer Aided Design-Computer Aided Manufacturing (CAD/CAM) and manual wiring diagrams; top-level assembly drawings and detailed design drawings; parts lists, assembly breakdown lists; interface control documentation to describe the physical, functional, and performance interfaces; and hardware, software, and system-level performance requirements.

The contractor shall develop technical documentation for new and ongoing systems. Documentation shall include preparing or updating technical manual, user manuals, operation and maintenance manuals, standard manuals, style guides, test plans, test reports, implementation plans, recommendations, bulletins, outlines and white papers. The contractor shall develop documentation for information systems and associated interfacing systems.

The contractor shall develop and/or provide inputs to System Engineering Plans (SEPs), Engineering Implementation Plans (EIPs), Contractor Integrated Technical Information System Implementation Plans (CITIS_IPs), Site Telecommunications Engineering Development Plans (STEDPs) required for Navy communications sites, and other engineering documentation required to satisfy coordination and tasking for networks and communications system implementation.

The contractor shall prepare and provide inputs for Program Protection Plans which includes Security Classification Guide (SCG), Counterintelligence Support Plan and Information Assurance documentation.

The contractor shall support technical and programmatic reviews in preparation for Milestone Decisions and other program events.

3.5 Systems Engineering: Cyber Security Certification and Accreditation (C&A)

The contractor shall provide results, documentation, mitigation, schedules and plans to ensure the Information Assurance posture meets required policy and that required authorizations are obtained and maintained.

3.5.1 DoD Information Assurance Certification and Accreditation Process (DIACAP)

The contractor shall develop, review or modify Interim Authority To Test (IATT) approvals to allow systems to test in simulated operational environment; or to use live data for a specific time period when specific test objectives cannot be met in a test environment.

The contractor shall develop, review or modify Interim Authority to Operate (IATO) or Authority to Operate (ATO) approvals, through execution of DIACAP packages and provide support during collaboration of risk determination to achieve full package approval.

DIACAP packages include: DIACAP Scorecard; Navy System Identification Profile (SIP); C&A plan; system description, diagrams and topologies; description of protections in place both physical and internal; Ports, Protocols and Services (PPS) list; Logical Network Diagram (LND) description; interdependencies; test plans, schedules, environments, configurations, locations and results of the proposed tests (i.e. Security Scans, Security Technical Implementation Guides (STIGS) etc.); and a Plan of Actions and Milestones (POA&M). Additional items may be added by accrediting authorities.

The contractor shall input all artifacts into Enterprise Mission Assurance Support Service (eMASS) or current data base for tracking C&A compliance.

The contractor shall create documentation of Assessment and Authorization (A&A) that meet the submission requirements found within the Risk Management Framework (RMF). The contractor shall follow the RMF activities to ensure security controls are implemented and information system security policy is being followed.

The contractor shall ensure that security posture of the configuration baseline meets requirements stated in all applicable DoD/DoN security documents.

3.5.2 Security Controls and System Scanning Support

The contractor shall provide and document vulnerability assessments to identify weaknesses in the system that can be exploited and mitigations to overcome them are documented in a POA&M. Assessments shall be of system design, development, production or operations relating to network infrastructure. The contractor shall conduct Certification Test & Evaluation (CT&E) and Security Test & Evaluation (ST&E) on networks and connected devices to determine whether all applicable Security Controls are satisfied, and findings are corrected, remediated or mitigated.

The contractor shall ensure all applicable Information Assurance Vulnerability Alerts (IAVAs) have been addressed and security updates are current; and remediate additional findings discovered during testing or received through agency announcements.

3.5.3 Cyber and Multi-Domain Systems

The contractor shall provide engineering and technical services to develop systems which will operate across the cyber domain to allow Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) of vital and time-sensitive data.

The contractor shall support engineering development for networks and systems across multiple security enclaves up to and including the TS/SCI Level. The contractor shall be able to achieve data transport, sharing and

interoperability across multiple security domains using message guards or switches, including multi-user connectivity from data servers.

3.6 Systems Engineering: Developmental Testing

The contractor shall perform and/or participate in testing of hardware and/or software developed by contractor or government developers in government designated facilities, test ranges, planned exercises or field tests.

The contractor shall support test director in monitoring, measuring, recording and reporting events incorporated in planned testing, including Test Readiness Reviews (TRRs). The contractor shall participate in Developmental Test & Evaluation (DT&E), and document test results of enterprise-wide systems, information systems, network components, equipment, and subsystems with interfacing C4ISR systems aboard ships, submarines, aircraft, unmanned systems and shore facilities. The contractor shall analyze and identify causes of problems and failures and report corrective actions or measures. The contractor shall support Operational Assessments (OAs).

3.7 Systems Engineering: Production

The contractor shall support Low-Rate Initial Production (LRIP), Full-Rate Production (FRP), Full-Rate Deployment (FRD) preparation and planning. The LRIP, FRP/D production requirements include EMP-hardening; TEMPEST-certification; and/or environmental testing (dust, heat, shock, vibration, humidity, etc.); and electromagnetic or similar physical parameters.

3.8 Systems Engineering: Operational Testing and Evaluation

The contractor shall support Operational Test and Evaluation (OT&E) and Follow-on OT&E (FOT&E) and all other types of testing mandated to achieve full deployment or fielding.

The contractor shall support evaluation of effectiveness, suitability and/or survivability.

3.9 Systems Engineering: Training

The contractor shall prepare training curricula, student and instructor guides, and related training materials. Conduct training courses in classroom and operational environments. Conduct system operational training.

3.10 Systems Engineering: Production Documentation and Reviews

3.10.1 Configuration Support

The contractor shall complete and finalize all documentation required for system production and deployment, include schematics, architectures, interface drawings, and configuration management data.

The contractor shall develop, implement and maintain configuration management, including configuration audit plans covering hardware and software in an integrated approach. The contractor shall verify and maintain complete and accurate configuration identification of each Configuration Item (CI) or Computer Software Configuration Item (CSCI) and government-approved established Functional, Allocated, and Product baselines for equipment or systems.

3.10.2 Baseline Documents and Databases

The contractor shall draft and update baseline documents related to systems engineering which include system concepts, system configurations, specifications, reports, accreditation documents, line drawings, Standard Operating Procedures (SOPs), architecture drawings, equipment lists and Bill of Materials (BoMs), manufacturing processes or procedures, test and inspection plans or procedures, surveys, quality assurance provisions, inspection and test equipment requirements, packaging lists, software documentation, technical manuals, training manuals, maintenance and supply documentation. The contractor shall input or update similar information in established databases for retention, tracking or maintenance of critical information and configurations.

3.10.3 Configuration Status Accounting

The contractor shall provide configuration status accounting, which shall delineate the status of changes from the baseline, the status of proposed changes, and the status of implementation of approved changes. The contractor may use the government-approved Automated Data Processing (ADP) system(s) for configuration status accounting. Configuration accounting shall be achieved through utilization of CMPro database, as used by SPAWAR.

3.10.4 Reviews

The contractor shall support technical, programmatic, production and/or sustainment planning meetings or reviews.

3.11 Systems Engineering: Installation

The contractor shall support site visits, develop site in-briefs and out-briefs, develop site survey checklists, generate installation schedules and identify potential risks.

The contractor shall prepare installation plans, Fleet Readiness Certification Board (FRCB) submissions, Base Electronic System Engineering Plans (BESEPs), Shipboard Alteration (SHIPALT) packages, and plans supporting certifications or approvals that are incidental to the system installation. The contractor shall be able to evaluate operational impact due to planned installations and advise on best course of action to minimize disruptions. The contractor shall provide input to, review and modify Installation Design Plans (IDPs) as required for FRCB submission. IDP shall include as block diagram, rack elevations, HVAC and power calculation, cabling and connector information, BoM, cable running sheets, final as-built drawings and all other required installation documentation.

The contractor shall generate, identify and verify material lists or BoMs, deliver required equipment and incidental materials necessary to complete the site installation, system integration or upgrade.

The contractor shall perform installation and integration of components or equipment, subsystems, systems, and networks in facilities, ships, submarines, aircraft or unmanned platforms. The contractor shall perform testing and troubleshooting to determine whether the installation has met stated objectives, and perform any corrections or modifications required to achieve full functionality and installation requirements.

The contractor shall support in the planning and execution of System Operational Verification Tests (SOVTs) as the final check-out demonstrating a successful, functional installation.

3.12 Systems Engineering: Operational Support to Platforms or Facilities

The contractor shall participate in the maintenance and support of platforms or facilities to ensure continued operations, including following logistics support plans to ensure parts and repair functions will meet required system availability requirements.

The contractor shall perform Communications Security (COMSEC) field and operability support, system configuration testing support, troubleshooting at the component to device level, software loading and updating, system monitoring and failure analysis, and recommendations for improved reliability.

The contractor shall provide system administration to address network and computer security updates and overall system security compliance.

3.13 Systems Engineering: Logistics Support

3.13.1 Integrated Logistics Support (ILS) Planning

The contractor shall develop and maintain Integrated Logistics Support Plan(s) (ILSP); User's Logistics Support Summary(s) (ULSS); Logistics Requirements and Funding Summary(s) (LRFS); Logistics Support Analysis Plan(s) (LSAP); Computer Resources Integrated Support Document (CRISD) and life cycle cost estimating. The impacts on all ILS elements shall be discussed in all ILS Plans, system engineering analyses and engineering change proposals. The ILS elements include the following: (1) Technical data; (2) Training and training support; (3) Maintenance; (4) Supply support; (5) Configuration management; (6) Support equipment; (7) Manpower and personnel; (8) Packaging, handling, storage and transportation; (9) Computer resources support; (10) Facilities; and (11) Design interface.

3.13.2 Logistic Support Analysis

The contractor shall perform Logistic Support Analysis (LSA) of systems supported by SSC Pacific Code 55100. The LSA process is iterative and may be continued through the life cycle of the systems to address engineering changes. These analyses shall include at a minimum: (1) identification of hardware or software for which the Government will not or may not receive full rights due to constraints imposed by regulations or laws limiting the information that must be furnished because of proprietary or other source control considerations; (2) development of supportability, cost, and readiness objectives including risk assessment; and (3) development of supportability related to design constraints for inclusion in specification(s) and other requirement documents.

3.14 Systems Engineering: Upgrades

The contractor shall provide system modernization support through technical inputs, participation in system modernization planning.

The contractor shall utilize Enterprise Change Request (ECR), Enterprise Change Notice (ECN), Engineering Change Proposal (ECP), Request for Change (RFC), Request for Deviation (RFD), or Request for Waiver (RFW) as

a process and control mechanism to implement upgrades and improvements to operational systems, and support the efforts necessary to complete these processes.

The contractor shall provide analysis and problem resolution study results supporting the improvement of specified networks, communication or information systems. The contractor shall provide inputs to system integration and interoperability requirements for new or enhanced COTS/GOTS products. The contractor shall provide reports showing the impacts of changes to baseline hardware and software.

3.15 Systems Engineering: Program and Project Management Support

The contractor shall provide technical and programmatic input and participate in the development of the Integrated Defense Acquisition, Technology and Logistics Life Cycle Management Framework for Navy, Joint and Coalition communications and networked systems.

The contractor shall participate in technical working group, technical interchange and integrated product team (IPT) planning meetings, preparing briefs and keeping meeting minutes and meeting artifacts. The contractor shall work with, and advise on process improvement.

3.16 Network and Computer Support

3.16.1 Network Systems Maintenance (for SSC Pacific)

The contractor shall provide network system maintenance and administration support. Including software and hardware maintenance, system integration and systems interface support of the systems.

The contractor shall provide analysis and administration support to projects requiring access to IT data, including design, development, and maintenance of tables; creation and maintenance of data dictionaries; and creation of bridges to populate new tables; file transfer and reformatting, troubleshooting, error investigation and correction, and production of specialized internal reports.

The contractor shall perform network system maintenance and quality assurance through validation and the integrity of access capability for operational and management query and reporting.

3.16.2 Network Operations Support

The contractor shall provide operations support for the networks of systems or projects that are outside the scope of the Navy/Marine Corps Internet (NMCI).

The contractor shall support the operation and troubleshooting of existing and deployed network systems. The contractor shall monitor internal and external network parameters and be able to work with the following technologies: synchronous and asynchronous protocols, Ethernet, FDDI, twisted pair, fiber optic, broadband Telephone Company (TELCO) (56kb, T1, T3) ATM, and emerging communication methodologies.

The contractor shall perform network database management support; perform network monitoring and statistical analysis; network control; and test equipment operation support.

The contractor shall provide upgrade development and implementation support for Gigabit-capable Passive Optical Networks (GPON) that includes implementation for data, voice, and video.

The contractor shall support virtualized network operations.

The contractor shall provide network contingency support; technical inputs; participate in network contingency planning; and provide execution support.

3.16.3 Network Timing Support

The contractor shall provide network timing support for all network systems utilizing current and future timing technologies.

Network timing systems shall utilize a Selective Availability/Anti Spoofing Module (SAASM)- Global Positioning System (GPS) based timing reference to be integrated into the specified Network(s). The intent is to provide a redundant Stratum Level 1 based distributed timing architecture across the network for client side equipment requiring frequency based clock reference and RFC 1305 Network Timing Protocol (NTP) version 4.0 for network-based time of day delivery.

3.16.4 Computer Operations Support

The contractor shall provide computer operations and maintenance for computer systems ranging from laptops to servers with operating systems used by DoD, including maintaining logs and records of jobs processed.

The contractor shall monitor systems for equipment failures, errors in performance, and security issues.

The contractor shall support virtualized computer operations.

The contractor shall reload systems after power outages and maintenance, perform backups, and restore files. The contractor shall install new software; software patches; security updates; and hardware based on project, program, or security requirements.

3.17 Process Improvement Planning

The contractor shall work collaboratively with SSC Pacific Code 55100 to establish and implement a Process Improvement Plan to improve the state of service management and engineering practices based on assessments of identified projects. The plan shall detail a logical set of activities to: (1) Improve service management and engineering processes to address the strengths and weaknesses of the organization identified in the initial appraisal; (2) Monitor progress throughout the improvement initiative; and (3) Rate the organization's maturity once a defined set of process areas have been improved. The plan shall delineate the appropriate Program Management Guide and CMMI process areas most applicable to the organization based on the initial appraisal; the objectives of the organization; and the availability of resources within the organization. Furthermore, the plan shall identify the processes for the organization to address within the CMMI for Services categories which are: Process Improvement, Project and Work Management, Support, Service Establishment and Delivery, and Engineering. The plan shall identify activities, resources and timeframes needed to execute critical improvement activities to help the organization prepare for appraisals.

3.18 Software

3.18.1 Application Integration and Application Development

Application Integration (AI) and Application Development (AD) are fundamental components of future Navy Systems in terms of both new development and support to legacy variants; where this effort specifically includes, but is not limited to, the following requirements and corresponds to Applicable Documents (provided at the task order level).

The contractor shall investigate, analyze and document application requirements in a feasibility assessment for each application, and shall provide the data needed for the CANES, Legacy and Application Integration engineering teams to ensure the Navy application provider's requirements are met.

The contractor shall review the System of System (SoS) architectures as designed and ensure alignment of applications with the CANES Functional Specification. Contractor shall provide recommended updates to either the application or the CANES Program technical documentation.

The contractor shall provide feedback and guidance to application providers regarding the AI Process including key dates, submission requirements, data requirements, test event schedules, and validate the application/system programmatic functional areas. The contractor shall work with the specific application providers to mitigate gaps and potential programmatic risks to integration.

The contractor shall work with application providers to investigate, define and document an integration solution, and ensure that the integration solution is aligned with Cyber Security and programmatic requirements IAW with applicable documents.

The contractor shall provide technical support by creating, updating and maintaining the existing AI documentation (i.e. HACSIM, AI Feasibility Assessments, and Service Request Forms) and clarification of integration solutions to application providers in support of fleet implementations.

The contractor shall develop applications to meet functionality define in programmatic requirement documents.

3.18.2 Software Development Planning

The contractor shall define a software development approach appropriate for the computer software effort to be performed under this solicitation. This approach shall be documented in a Software Development Plan (SDP). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

The SDP shall define the offeror's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE/EIA Std. 12207-2008. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207-2008, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. Because IEEE/EIA Std. 12207-2008 does not prescribe how to accomplish the task, the offeror must provide this detailed information so the Government can assess whether the offeror's approach is viable. In all cases, the level of detail shall be sufficient to define all software development

processes, activities, and tasks to be conducted. Information provided must include, as a minimum, specific standard, methods, tools, action, strategies, and responsibilities associated with development and qualification.

4.0 REPORTS, DATA and DELIVERABLES

4.1 Deliverables

Data deliverables will be specified in the Contract Data Requirements List (CDRL), DD 1423-1 for individual Delivery/Task Orders.

4.2 Contractor Manpower Reporting

The contractor shall report all contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Navy via a secure data collection website. The contractor is required to completely fill in all required data fields using the following web address <https://doncmra.nmci.navy.mil>. Reporting inputs will be for the labor executed during the period of performance on task orders for each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk at <http://www.ecmra.mil/>.

5.0 OTHER

5.1 Security

The security requirement for this tasking will be up to and including Top Secret and Sensitive Compartmented Information. The work performed by the Contractor will include access to unclassified and up to Top Secret/SCI data, information, meetings, and spaces. Individual task orders awarded under this basic contract will specify security clearance level required for contractor personnel. Individual task orders may require contract personnel to have access to Communications Security (COMSEC) material or be a COMSEC Material System (CMS) user. The security clearance of the contractor personnel assigned to the task order must be appropriate for the associated COMSEC material/equipment. Individual task orders may also require contract personnel to be North Atlantic Treaty Organization (NATO) briefed and complete the derivative classification training prior to being granted access to the Secure Internet Protocol Router Network (SIPRNet)/Joint Worldwide Intelligence Communications System (JWICS); training is provided by the facility security officer.

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI with ICD 704 eligibility (which replaced DCID 6/4 eligibility).

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to Commanding Officer, Attn: Foreign Travel Team, Space and Naval Warfare Systems Center Pacific, 53560 Hull Street, Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 40 days

in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at <https://atlevel1.dtic.mil/at/>, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863. SERE 100.1 Level A Code of Conduct training is also required prior to OConus travel for all personnel. SERE 100.1 Level A training can be accessed at <https://wwwa.nko.navy.mil>. Other specialized training for specific locations may also be required contact the SSC Pacific foreign travel team.

Applicable documents: SECNAVINST 5510.30 (Series), Department of Navy Personnel Security Program, 06/2006 SECNAVINST 5510.36 (Series), Department of Navy Information Security Program, 06/2006, OPNAVINST F3300.53C (Series), Navy Antiterrorism Program DOD 5200.01 Volumes 1 through 4 (Series), DOD Security Program, DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM)

Operations Security (OPSEC): OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

Applicable documents: National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298, 01/22/88, DOD 5205.02 (Series), DOD Operations Security (OPSEC) Program, 11/03/08, OPNAVINST 3432.1 (Series), DON Operations Security, 11/04/11, SPAWARINST 3432.1 (Series), Operations Security Policy, 02/02/05.

5.1.1 Network Access

Contractors, including sub-contractors, may require access to classified networks to perform and complete the work authorized under this contract. Access may include connectivity to Secret and SCI level networks (i.e. SIPRnet, JWICS, NSAnet, etc.), and may include access to web-sites, data bases, email or other applications deemed necessary. Network access is only required at government facilities.

5.2 Communication Security Material System

Communication Security Material System (CMS) access will be required for work on this contract.

5.3 Cyber Security Work Force

Cyber Security Work Force (CSWF) certifications are required for contractor personnel under this contract. All IA functions to be performed under this contract will be identified at the task order level in the performance work statement. Task order performance work statements will specify, as applicable, IA workforce category, level, training, and certification requirements for contractor personnel with privileged access working in IA Technical (IAT) environments, IA Management (IAM) personnel with significant IA tasks, Computer Network Defense Service Providers (CND-SPs), and IA Systems Architects and Engineers (IASAEs). Task orders with IA functions will include a requirement for the contractor to report IA certification status and compliance.

5.3.1 CSWF Personnel

The Contractor shall ensure personnel supporting this contract who are performing IA functions that are designated as IA Workforce positions IAW DoD 8570.01-M shall be trained and certified in accordance with DFARS Clause 252.239-7001 Information Assurance Contractor Training and Certification. The contractor shall follow SECNAVINST 5239.3A of 20 Dec 2004 & DoD 8500.2 of 6 Feb 2003 when performing IA tasks orders. The Contractor shall meet applicable information assurance certification requirements, including (1) DoD-approved IA workforce certifications appropriate for each specified category and level and (2) appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

5.3.2 CSWF Certifications

The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using a CDRL Contractor Roster, Data Item Description# DI-MGMT-81596, for individual task/delivery orders. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

End of PWS

CLAUSES INCORPORATED BY FULL TEXT

5252.204-9200 SECURITY REQUIREMENTS (DEC 1999)

The work to be performed under this contract as delineated in the DD Form 254, Attachment No. 1 involves access to and handling of classified material up to and including Top Secret SCI.

In addition to the requirements of the FAR 52.204-2 "Security Requirements" clause, the Contractor shall appoint a Security Officer, who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industry Security Program Operating Manual (DODINST 5220.22M), and (3) assure compliance with any written instructions from the Security Officer, Code 85003, 53560 Hull Street, San Diego, CA, 92152-5001.

(End of clause)

5252.216-9217 DELIVERY/TASK ORDER PROCEDURES (SEP 2014)—ALTERNATE II

The order procedures below are provided for informational purposes only. The actual procedures (including response times) may vary according to individual order circumstances.

(a) *Multiple Award Contract (MAC) Ordering Procedures.* It is anticipated that each competitive order will be placed in accordance with the following procedures:

In accordance with FAR 16.505(b)(2)(i)(F), the Government may set aside the competition for orders for small business concerns should the Government determine that the "rule of two" applies (see FAR 19.502-2). If there is only one small business awarded a prime MAC contract (along with large business MAC awardees), then the contracting officer also reserves the right to noncompetitively award an order to that small business concern.

(1) *Requirements Documentation.* Upon identification of a requirement, the cognizant technical code will develop a draft Performance Work Statement (PWS)/Statement of Work (SOW) and other requirements documents (e.g., Contract Data Requirements List (CDRL)) consistent with the technical requirements of this contract and the specific effort. Both level-of-effort (term) and completion type orders may be issued under this contract. Each order will include the order type deemed appropriate by the Government.

(2) *Draft RFP**. The contract specialist will issue a draft Request for Proposals (RFP) to all MAC contractors** which will include, at a minimum, the draft PWS/SOW, anticipated CDRL data items, and the anticipated selection procedures for the order. Contractors are strongly encouraged at this stage to ask questions pertaining to the draft RFP, such as regarding the Government's evaluation strategy, and to provide comments that could potentially help the Government improve the procurement. The time allotted for the submission of questions and/or comments is typically 2 to 5 business days.

*The Government may choose to skip the "Draft RFP" step altogether. In those instances, however, the contractors will still be allowed a question and answer period which will be identified in the RFP.

**Since correspondence is conducted via email, all MAC awardees are strongly encouraged to provide more than one email address to the Government to ensure that multiple contractor POCs receive the Government's emails. The Government reserves the right to not include large business prime contractors on correspondence relating to orders set aside for small business.

The Government desires more than one offeror to submit a proposal for each order. Contractors are strongly encouraged to provide a preliminary decision as to whether or not they intend to submit a proposal in response to the final RFP. Should a contractor decide not to submit a proposal for the order, the Government may request the contractor to provide documentation to the Government indicating the reason(s) why no proposal is being submitted. Additionally, the contractor is strongly encouraged to indicate if additional time to respond to the final RFP would cause the contractor to submit a proposal, and if so, how much additional time would be required. This initial propose/no-propose decision is strongly encouraged and is due no later than the deadline for questions and/or comments in response to the draft RFP.

(3) *Final RFP.* After the submission time for questions/comments in response to the draft RFP has expired, the Government will issue a final RFP which will contain the finalized requirements documents and selection procedures for the order. All eligible MAC awardees, even those that conveyed intent to not propose, will receive the final RFP. If there were any questions submitted during the draft RFP phase, at the Government's discretion, pertinent questions and answers (properly sanitized of proprietary information) will be distributed to all eligible MAC contractors along with the final RFP. The time allotted for the submission of proposals is typically 5 to 10 business days.

Contractors that provided an intent-to-propose at the draft RFP stage, and then subsequently decide NOT to submit a proposal, are strongly encouraged to provide the same level of detail as identified above regarding why they are choosing not to submit a proposal. Any subsequent propose/no-propose decision that conflicts with the initial propose/no-propose decision are strongly encouraged to be submitted to the Government as early as possible.

(4) *Source Selection Procedures.* For a given order, the selection procedures will be based on a best value process, whether allowing for a tradeoff process (see FAR 15.101-1) or a low price/cost, or lowest price technically acceptable process (see FAR 15.101-2); however, in accordance with FAR 16.505(b)(1)(ii), FAR 15.3 will not apply. Each RFP will provide instructions to the MAC contractors as to the specific procedures for responding to the RFP and describe what information shall be presented to the Government in order to be considered for award of the order. The Government reserves the right to clarify certain aspects of one or more of the proposals, without contacting all offerors, unless such communication is used to materially alter the technical or cost elements and/or otherwise revise the proposal.

(5) *Evaluation and Award.* The Government will evaluate proposals and make award based on the evaluation criteria set forth in the final RFP. Once an offeror's proposal has been selected for award, a DD Form 1155 will be executed by the Contracting Officer and sent to the contractor via e-mail or facsimile as notice to begin work. The contractor is cautioned that no work is to be started prior to receipt of a properly signed and executed DD Form 1155, Order for Supplies/Services, or other authorization by the Contracting Officer.

Within a reasonable amount of time (usually within 1 business day) after order award, the name of the awardee and the total value of the order will be provided to all MAC contractors.

(b) *Non-Competitive Ordering Procedures.* It is anticipated that each order awarded to a single award contractor, or to a MAC contractor when a Contracting Officer-approved exception at FAR 16.505(b)(2)(i)(A) through (F) applies, or when making a Contracting Officer-approved award to a small business as outlined above, will be placed in accordance with the following procedures:

(1) *Requirements Documentation.* Upon identification of a requirement, the cognizant technical code will develop a draft PWS/SOW and other requirements documents (e.g., CDRL) consistent with the technical requirements of the effort. Both level of effort (term) and completion type orders may be issued under this contract. The PWS/SOW will include the order type deemed appropriate by the Government.

After both parties have reached agreement regarding the technical requirements of the PWS/SOW, the contractor and the Contracting Officer's Representative (COR) shall sign and date the final document to signify their common understanding of the order requirements.

(2) *Cost Estimate**. Typically within 1 to 5 business days after signing the PWS/SOW, the contractor will submit to the contract specialist and the COR/COR Support Manager (CSM) a complete cost estimate. The cost estimate shall contain the following information to enable the Contracting Officer to make a determination of cost/price reasonableness:

(i) Individually listed labor categories, direct labor hours, and unburdened hourly labor rates for each labor category. Unless proposing a new labor category not listed in the basic contract, all proposed labor categories should either exactly match, or be mapped to the labor categories identified in the basic solicitation.

(ii) Other Direct Cost (ODC) cost information shall include identification of: 1) material (consumable and non-consumables) purchase description and amount; 2) summary of travel costs to include identification of number of travelers, destination, and duration for each trip and 3) other direct costs not separately identified.

(iii) Actual indirect rates used and note their application.

(iv) Show totals for individual cost elements, as well as the overall total for hours, estimated cost, and cost plus fee. Identify the average hourly labor rate for the overall proposal (computed by dividing total fully burdened labor cost by total labor hours).

(v) If applicable, subcontractor costs, names of subcontractor(s) and type of subcontract(s).

(vi) For proposed personnel, identify the fully burdened hourly labor rate inclusive of all applicable indirect costs and fee.

****These cost estimate elements apply to both competitive and non-competitive orders.***

(3) *Cost Evaluation and Award*. Once the Contracting Officer has reviewed and accepted the contractor's cost estimate, a DD Form 1155 will be executed by the Contracting Officer and sent to the contractor via e-mail or facsimile as notice to begin work. The contractor is cautioned that no work is to be started prior to receipt of a properly signed and executed DD Form 1155, Order for Supplies/Services, or other authorization by the Contracting Officer. As necessary, the contract administrator or contracting officer will contact the contractor to negotiate costs or minor requirements details before a DD Form 1155 is executed.

(c) *Content*. All orders will include the following elements:

- (1) Effective date of order
- (2) Contract and order numbers
- (3) Type of order (i.e., completion or level-of-effort-term)
- (4) Estimated hours
- (5) Estimated cost, fee or price
- (6) Scope
- (7) Inspection and Acceptance Terms

(8) Delivery and/or period of performance (PoP) dates

(9) Place of delivery or performance

(10) Accounting and appropriation data

(11) Other information as appropriate (e.g., COR Designation, Government Furnished Property, material, or facilities to be made available for performance of the order; safety requirements; security requirements set forth on DD Form 254; data requirements set forth on DD Form 1423).

(12) Each order under a cost-reimbursement contract is deemed to include the clause at FAR 52.232-20 "Limitation of Cost" or 52.232-22 "Limitation of Funds," whichever is applicable.

(d) *Contractor Notification.* The contractor is responsible for immediately notifying the Contracting Officer of any difficulties in performing in accordance with the terms of the order.

(e) *Competition Advocate.* For this contract, the designated order ombudsman is the Navy Competition Advocate General (DASN (AP) as per NMCARS 5206.501). The ombudsman is responsible for reviewing complaints from multiple award contractors and ensuring that all of the contractors are afforded a fair opportunity to be considered for orders in excess of \$3,000, consistent with procedures in the contract. However, it is not within the designated ombudsman's authority to prevent the issuance of an order or to disturb an existing order. Contractors are encouraged to settle their complaints through the Competition Advocate chain of command, seeking review by the Competition Advocate at SSC Pacific, Code 20

(<http://www.public.navy.mil/spawar/Pacific/22000/Pages/ContactUs.aspx>) before taking complaints to the Navy Competition Advocate General.

(End of clause)

5252.222-9201 WORK WEEK (SSC-PAC) (APR 2012)

(a) All or a portion of the effort under this contract will be performed on a Government installation. The normal work week for Government employees at the Space and Naval Warfare Systems Center Pacific (SPAWARSYSCEN Pacific) is Monday through Thursday 7:15 AM to 4:45 PM and Friday 7:15 AM to 3:45 PM with every other Friday a non-work day. Work at this Government installation, shall be performed by the contractor within the normal work hours at SPAWARSYSCEN Pacific unless differing hours are specified on the individual delivery/task orders. The Contractor is not required to maintain the same hours as Government employees; however, contractor employees performing work at SPAWARSYSCEN Pacific must work during the normal workweek. The following is a list of holidays observed by the Government.

<u>Name of Holiday</u>	<u>Time of Observance</u>
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
Presidents Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October

Veteran's Day
Thanksgiving Day
Christmas Day

11 November
Fourth Thursday in November
25 December

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the Contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the Contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations the payment of overtime is required only when an employee works more than 40 hours during a week. Therefore, during the SPAWARSYSCEN Pacific off-Friday (36 hour) week overtime will not be paid for non-exempt employees. During the work-Friday week (44 hour) the contractor is to schedule work so as not to incur overtime charges during the normal work week unless authorized in writing by the Government to do so. An example of this would be for contractor personnel to work during the hours of 7:45 AM to 4:15 PM Monday through Thursday and 7:15 AM to 3:45 PM Friday during the work-Friday week. The contractor may also elect to configure the workforce in such a way that no single employee exceeds 40 hours during a normal week even though normal SPAWARSYSCEN Pacific hours are maintained both weeks.

(e) Periodically the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises which may require the Contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The Contractor will be required to work with its Government point of contact to adjust work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours, or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

(End of clause)

5252.223-9200 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS (NOV 2008)

(a) If performance of any work under this contract is required at a SPAWAR Systems Center Pacific facility, the Contractor shall contact the Safety and Environmental Office, Code 83500 at 619-553-5024 prior to performance of ANY work under this contract. *The purpose of contacting the Safety and Environmental Office is to obtain and become familiar with any local safety regulations or instructions and to inform the local Safety Officer of any work taking place on base.* **Safety and Occupational Health personnel cannot assume a regulatory role relative to oversight of the contractor safety activities and performance except in an imminent danger situation. Administrative oversight of contractors is the primary responsibility of the Contracting Officer and/or the Contracting Officer's designated representative.**

(b) Contractors are responsible for following all safety and health related State and Federal statutes and corresponding State, Federal and/or Navy regulations protecting the environment, contractor employees, and persons who live and work in and around contractor and/or federal facilities.

(c) Contractors shall monitor their employees and ensure that they are following all safety regulations particular to the work areas. Contractors shall ensure that their employees (i) wear appropriate safety equipment and clothing,

(ii) are familiar with all relevant emergency procedures should an accident occur, and (iii) have access to a telephone and telephone numbers, to include emergency telephone numbers, for the SPAWAR Systems Center Pacific facility where work is performed.

(End of clause)

5252.227-9211 PROCEDURES FOR CONTROLLING TECHNICAL DOCUMENTS UNDER SPAWARSCEN PACIFIC CONTRACTS (NOV 2008)

The Contractor shall comply with DOD Directive 5230.25 and the information provided herein when the Government provides the Contractor with technical data.

(a) Location of distribution statement, export warning notice, and destruction notice (classified and unclassified technical documents).

- (1) Standard written or printed material with covers and/or title pages: Statement(s) to be printed, typed, or stamped on the front cover and title page.
- (2) Technical documents without covers or title pages: Statement(s) to be typed, printed, or stamped on the first page of the document.
- (3) Deck of punched or aperture cards: Statement(s) to be typed, printed, or stamped on face of first and last card and on top of deck.
- (4) Magnetic tape, cassette, or disk: Statement(s) to be typed, stamped, or printed on a label applied to outside of material. The first page of the resulting hard-copy report or computer printout is also marked with applicable statement(s).
- (5) Microfilm: Statement(s) to be typed, stamped, or printed on outside of jacket or canister housing the material. The first page of the resulting hard-copy report or first frame is also marked with applicable statement(s). The headers for microfiche must carry an abbreviated version of the statement(s).
- (6) Drawings: Applicable statement(s) to be typed, stamped, or printed near the title block.

(b) Safeguarding of Unclassified, Limited-Access Documents (for classified documents see SSCPACINST 5500.1B).

- (1) Normal working hours: Limited-access documents and those that have not yet been reviewed cannot be left unattended in work areas accessible to non-DoD employees.
- (2) After normal working hours: Limited-access documents and those that have not yet been reviewed should be placed in locked files, desks, or similar containers. If this is not possible, locked offices or buildings are adequate.
- (3) Additional guidance for safeguarding limited-access media processed by an IT system, activity, or network can be found in OPNAVINST 5239.1A.

(c) Destruction of Unclassified, Limited-Access Documents. Destroy by any method that will prevent disclosure of contents or reconstruction of the material. Examples of such destruction methods follow:

- (1) Printed document, deck of punched or aperture cards, computer printout, and drawings: Destroy by tearing each copy into pieces to preclude reconstruction and placing the pieces in regular trash containers or send to the Mail Room Branch for destruction.
- (2) Magnetic tape, cassette, or disk: Destroy by erasing the magnetic storage media.
- (3) Microfilm: Destroy by cutting into small pieces or send to the mailroom for destruction.

(d) Safeguarding of Classified Documents: See SSCPACINST 5500.1B.

(e) Destruction of Classified Documents: See SSCPACINST 5500.1B.

(End of specification)

5252.228-9201 LIABILITY INSURANCE--COST TYPE CONTRACTS (OCT 2001)

(a) The following types of insurance are required in accordance with the FAR 52.228-7 "Insurance--Liability to Third Persons" clause and shall be maintained in the minimum amounts shown:

- (1) Workers' compensation and employers' liability: minimum of \$100,000
- (2) Comprehensive general liability: \$500,000 per occurrence
- (3) Automobile liability: \$200,000 per person
\$500,000 per occurrence
\$ 20,000 per occurrence for property damage

(b) When requested by the contracting officer, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

(End of clause)

Section D - Packaging and Marking

TBD

To be Determined at the Task Order level.

Section E - Inspection and Acceptance

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
0002	Destination	Government	Destination	Government
1001	Destination	Government	Destination	Government
1002	Destination	Government	Destination	Government
2001	Destination	Government	Destination	Government
2002	Destination	Government	Destination	Government

CLAUSES INCORPORATED BY REFERENCE

52.246-5	Inspection Of Services Cost-Reimbursement	APR 1984
52.246-9	Inspection Of Research And Development (Short Form)	APR 1984

Section F - Deliveries or Performance

DELIVERY INFORMATION

CLIN	ORDERING PERIOD	QUANTITY	SHIP TO ADDRESS
0001	36 Months After Date of Contract Award	N/A	N/A, FOB DESTINATION
0002	36 Months After Date of Contract Award	N/A	N/A, FOB DESTINATION
1001	12 Months After Date of Option I (if exercised by the Government)	N/A	N/A, FOB DESTINATION
1002	12 Months After Date of Option I (if exercised by the Government)	N/A	N/A, FOB DESTINATION
2001	12 Months After Date of Option II (if exercised by the Government)	N/A	N/A, FOB DESTINATION
2002	12 Months After Date of Option II (if exercised by the Government)	N/A	N/A, FOB DESTINATION

CLAUSES INCORPORATED BY REFERENCE

52.242-15	Stop-Work Order	AUG 1989
52.242-15 Alt I	Stop-Work Order (Aug 1989) - Alternate I	APR 1984
52.247-34	F.O.B. Destination	NOV 1991

Section G - Contract Administration Data

CLAUSES INCORPORATED BY FULL TEXT

252.204-7006 BILLING INSTRUCTIONS (OCT 2005)

When submitting a request for payment, the Contractor shall--

- (a) Identify the contract line item(s) on the payment request that reasonably reflect contract work performance; and
- (b) Separately identify a payment amount for each contract line item included in the payment request.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

- (a) Definitions. As used in this clause--

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.

- (b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

- (c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the System for Award Management at <https://www.acquisition.gov>; and

(2) Be registered to use WAWF at <https://wawf.eb.mil/> following the step-by-step procedures for self-registration available at this Web site.

- (d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at <https://wawf.eb.mil/>.

(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).

Cost Voucher (FAR 52.216-7)

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

Not Applicable

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	HQ0338 (DFAS)
Issue By DoDAAC	N66001
Admin DoDAAC	S1103A (DCMA)
Inspect By DoDAAC	Not Applicable
Ship To Code	Not Applicable
Ship From Code	Not Applicable
Mark For Code	Not Applicable
Service Approver (DoDAAC)	HAA110 (DCAA) on interim vouchers (and HAA110 DCAA and S1103A (DCMA) on final voucher)
Service Acceptor (DoDAAC)	To be Determined
Accept at Other DoDAAC	Not Applicable
LPO DoDAAC	Not Applicable
DCAA Auditor DoDAAC	HAA110 (DCAA)
Other DoDAAC(s)	Not Applicable

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the email address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.

The COR's email address will be specified at the Task Order level.

(g) WAWF point of contact.

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

Not Applicable

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

(End of clause)

5252.201-9201 DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE (MAR 2006)

(a) The Contracting Officer hereby appoints the following individual as Contracting Officer's Representative(s) (COR) for this contract/order:

CONTRACTING OFFICER REPRESENTATIVE

Name: *

Code: *

Address: *

Phone Number: *

E-mail: *

*To be determined at the Task Order level.

(b) It is emphasized that only the Contracting Officer has the authority to modify the terms of the contract, therefore, in no event will any understanding agreement, modification, change order, or other matter deviating from the terms of the basic contract between the Contractor and any other person be effective or binding on the Government. When/If, in the opinion of the Contractor, an effort outside the existing scope of the contract is requested, the Contractor shall promptly notify the PCO in writing. No action shall be taken by the Contractor unless the Procuring Contracting Officer (PCO) or the Administrative Contracting Officer (ACO) has issued a contractual change.

(End of Clause)

CLAUSES INCORPORATED BY FULL TEXT

5252.216-9209 APPOINTMENT OF ORDERING OFFICER(S) (DEC 1999)

(a) The contracting officer and/or his duly authorized representative at the following activity(ies) are designated as Ordering Officers:

Name: Any Warranted Contracting Officer

Activity: SPAWAR Systems Center Pacific

(b) The above individual(s) is/are responsible for issuing and administering any orders placed hereunder. Ordering Officers may negotiate revisions/modifications to orders, but only within the scope of this contract. Ordering Officers have no authority to modify any provision of this basic contract. Any deviation from the terms of the basic contract must be submitted to the Procuring Contracting Officer (PCO) for contractual action. Ordering Officers may enter into mutual no-cost cancellations of orders under this contract and may reduce the scope of orders/tasks, but Terminations for Convenience or Terminations for Default shall be issued only by the PCO.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

5252.216-9210 TYPE OF CONTRACT (DEC 1999)

This is a Cost-Plus-Fixed-Fee (CPFF) contract.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

5252.227-9213 PATENT MATTERS POINT OF CONTACT (OCT 2008)

The Point of Contact regarding Patent Matters for this contract is:

OFFICE OF PATENT COUNSEL / CODE 360012
SPAWARSYSCEN
53560 HULL STREET
SAN DIEGO, CA 92152-5001
(619) 553-3001

Do not submit interim and final invention reports to this address. See the clause at 5252.227-9206 for the proper address.

(End of clause)

5252.232-9206 SEGREGATION OF COSTS (DEC 2003)

(a) The Contractor agrees to segregate costs incurred under this contract at the lowest level of performance, either task or subtask, rather than on a total contract basis, and to submit invoices reflecting costs incurred at that level. Invoices shall contain summaries of work charged during the period covered, as well as overall cumulative summaries by labor category for all work invoiced to date, by line item, task or subtask.

(b) Where multiple lines of accounting are present, the ACRN preceding the accounting citation will be found in Section B and/or Section G of the contract or in the task or delivery order that authorizes work. Payment of Contractor invoices shall be accomplished only by charging the ACRN that corresponds to the work invoiced.

(c) Except when payment requests are submitted electronically as specified in the clause at DFARS 252.232-7003, Electronic Submission of Payment Requests, one copy of each invoice or voucher will be provided, at the time of submission to DCAA:

- (1) to the Contracting Officer's Representative or the Technical Representative of the Contracting Officer, and
- (2) to the Procuring Contracting Officer.

(End of clause)

WAWF

SUPPLEMENTAL WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS

(a) The following Wide Area WorkFlow (WAWF) payment instructions supplement DFARS Clause 252.232-7006.

(b) Interim Voucher costs are to be broken down in a clear and logical manner with fully burdened cost information (inclusive of fee). Cost information shall include identification of: 1) all labor categories and individuals utilized during the billing period; 2) number of hours and fully burdened hourly labor rates (including fee) per individual*; 3) material (consumable and non-consumables) description and fully burdened costs, separated by type; 4) fully burdened travel costs itemized by trip, date and individual; 5) other fully burdened direct costs not separately identified; e.g., reproduction, cell phones, equipment rentals, etc.; 6) subcontractor costs itemized with the same level of detail; and 7) average actual hourly labor rates (total actual fully burdened labor cost/total # hrs performed).

*In lieu of providing names of individuals, you may choose to assign an "employee code" to each individual. If the aforementioned methodology is chosen the Contracting Officer may require an employee matrix mapping the employee codes to an individual name.

Attachments created with any Microsoft Office product or Adobe (.pdf files) are to be attached to the invoice in WAWF. The total size limit for files per invoice in WAWF is 5 megabytes. A separate copy of the invoice with back-up documentation shall be emailed to the COR/TOM.

(c) Contractors approved by DCAA for direct billing will not process vouchers through DCAA, but will submit directly to DFAS. Vendors MUST still provide a copy of the invoice and any applicable cost back-up documentation supporting payment to the Acceptor/Contracting Officer's Representative (COR) if applicable. Additionally, a copy of the invoice(s) and attachment(s) at time of submission in WAWF shall also be provided to each point of contact identified in section (g) of DFARS clause 252.232-7006 by email. If the invoice and/or receiving report are delivered in the email as an attachment it must be provided as an Adobe (.pdf file), Microsoft Office product or other mutually agreed upon form between the Contracting Officer and vendor.

(d) A separate invoice will be prepared no more frequently than for every two weeks. Do not combine the payment claims for services provided under this contract.

(e) In accordance with DFARS 204.7104-1 Informational subline item numbers (e.g., 000101, 000102, etc.) shall not be priced separately for payment purposes. Therefore, you are reminded to bill at the CLIN level using the applicable ACRN, e.g., AA, AB, AC, etc. DFAS will reject invoices that contain informational subline items.

(End of instruction)

Section H - Special Contract Requirements

CLAUSES INCORPORATED BY FULL TEXT

252.234-7002 EARNED VALUE MANAGEMENT SYSTEM (DEVIATION) (SEP 2015)

Note: This clause is only applicable at the task order level, when the task order is valued over \$20,000,000.00 and when specified by the Contracting Officer.

(a) Definitions. As used in this clause--

“Acceptable earned value management system” means an earned value management system that generally complies with system criteria in paragraph (b) of this clause.

“Earned value management system” means an earned value management system that complies with the earned value management system guidelines in the ANSI/EIA-748.

“Significant deficiency” means a shortcoming in the system that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes.

(b) System criteria. In the performance of this contract, the Contractor shall use--

(1) An Earned Value Management System (EVMS) that complies with the EVMS guidelines in the American National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748); and

(2) Management procedures that provide for generation of timely, reliable, and verifiable information for the Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) required by the CPR and IMS data items of this contract.

(c) If this contract has a value of \$100 million or more, the Contractor shall use an EVMS that has been determined to be acceptable by the Cognizant Federal Agency (CFA). If, at the time of award, the Contractor's EVMS has not been determined by the CFA to be in compliance with the EVMS guidelines as stated in paragraph (b)(1) of this clause, the Contractor shall apply its current system to the contract and shall take necessary actions to meet the milestones in the Contractor's EVMS plan.

(d) If this contract has a value of less than \$100 million, the Government will not make a formal determination that the Contractor's EVMS complies with the EVMS guidelines in ANSI/EIA-748 with respect to the contract. The use of the Contractor's EVMS for this contract does not imply a Government determination of the Contractor's compliance with the EVMS guidelines in ANSI/EIA-748 for application to future contracts. The Government will allow the use of a Contractor's EVMS that has been formally reviewed and determined by the CFA to be in compliance with the EVMS guidelines in ANSI/EIA-748.

(e) The Contractor shall submit notification of any proposed substantive changes to the EVMS procedures and the impact of those changes to the CFA. If this contract has a value of \$100 million or more, unless a waiver is granted by the CFA, any EVMS changes proposed by the Contractor require approval of the CFA prior to implementation. The CFA will advise the Contractor of the acceptability of such changes as soon as practicable (generally within 30 calendar days) after receipt of the Contractor's notice of proposed changes. If the CFA waives the advance approval requirements, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(f) The Government will schedule integrated baseline reviews as early as practicable, and the review process will be conducted not later than 180 calendar days after--

- (1) Contract award;
- (2) The exercise of significant contract options; and
- (3) The incorporation of major modifications.

During such reviews, the Government and the Contractor will jointly assess the Contractor's baseline to be used for performance measurement to ensure complete coverage of the statement of work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.

(g) The Contractor shall provide access to all pertinent records and data requested by the Contracting Officer or duly authorized representative as necessary to permit Government surveillance to ensure that the EVMS complies, and continues to comply, with the performance criteria referenced in paragraph (b) of this clause.

(h) When indicated by contract performance, the Contractor shall submit a request for approval to initiate an over-target baseline or over-target schedule to the Contracting Officer. The request shall include a top-level projection of cost and/or schedule growth, a determination of whether or not performance variances will be retained, and a schedule of implementation for the rebaselining. The Government will acknowledge receipt of the request in a timely manner (generally within 30 calendar days).

(i) Significant deficiencies.

(1) The Contracting Officer will provide an initial determination to the contractor, in writing, on any significant deficiencies. The initial determination will describe the deficiency in sufficient detail to allow the Contractor to understand the deficiency.

(2) The Contractor shall respond within 30 days to a written initial determination from the Contracting Officer that identifies significant deficiencies in the Contractor's EVMS. If the Contractor disagrees with the initial determination, the Contractor shall state, in writing, its rationale for disagreeing.

(3) The Contracting Officer will evaluate the Contractor's response and notify the Contractor, in writing, of the Contracting Officer's final determination concerning--

(i) Remaining significant deficiencies;

(ii) The adequacy of any proposed or completed corrective action;

(iii) System noncompliance, when the Contractor's existing EVMS fails to comply with the earned value management system guidelines in the ANSI/EIA-748; and

(iv) System disapproval, if initial EVMS validation is not successfully completed within the timeframe approved by the Contracting Officer, or if the Contracting Officer determines that the Contractor's earned value management system contains one or more significant deficiencies in high-risk guidelines in ANSI/EIA-748 standards (guidelines 1, 3, 6, 7, 8, 9, 10, 12, 16, 21, 23, 26, 27, 28, 30, or 32). When the Contracting Officer determines that the existing earned value management system contains one or more significant deficiencies in one or more of the remaining 16 guidelines in ANSI/EIA-748 standards, the contracting officer will use discretion to disapprove the system based on input received from functional specialists and the auditor.

(4) If the Contractor receives the Contracting Officer's final determination of significant deficiencies, the Contractor shall, within 45 days of receipt of the final determination, either correct the significant deficiencies or submit an acceptable corrective action plan showing milestones and actions to eliminate the significant deficiencies.

(j) Withholding payments. If the Contracting Officer makes a final determination to disapprove the Contractor's EVMS, and the contract includes the clause at 252.242-7005, Contractor Business Systems, the Contracting Officer will withhold payments in accordance with that clause.

(k) With the exception of paragraphs (i) and (j) of this clause, the Contractor shall require its subcontractors to comply with EVMS requirements as follows:

(1) For subcontracts valued at \$100 million or more, the following subcontractors shall comply with the requirements of this clause:

Not Applicable.

(2) For subcontracts valued at less than \$100 million, the following subcontractors shall comply with the requirements of this clause, excluding the requirements of paragraph (c) of this clause:

Not Applicable.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

252.239-7001 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION (JAN 2008)

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including--

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

5252.204-9202 CONTRACTOR PICTURE BADGE (DEC 1999)

(a) A contractor picture badge may be issued to contractor personnel by the SSC Pacific Badge and Decal Office (<http://www.public.navy.mil/spawar/Pacific/Pages/VisitorInformation.aspx>) upon receipt of a valid visit request from the Contractor and a picture badge request from the COR. A list of personnel requiring picture badges must be provided to the COR to verify that the contract or delivery/task order authorizes performance at SSC Pacific prior to completion of the picture badge request..

(b) The contractor assumes full responsibility for the proper use of the identification badge and automobile decal, and shall be responsible for the return of the badge and/or destruction of the automobile decal upon termination of personnel or expiration or completion of the contract.

(c) At the completion of the contract, the contractor shall forward to the SSC Pacific Badge and Decal Office a list of all unreturned badges with a written explanation of any missing badges.

(End of clause)

5252.209-9201 ORGANIZATIONAL CONFLICT OF INTEREST (SYSTEMS ENGINEERING) (DEC 1999)

(a) This contract provides for systems engineering and related technical support for Networks and Communications Division (Code 551) engineering support described in the PWS. The parties recognize that by the Contractor providing this support, a potential conflict of interest arises as defined by FAR 9.505-1.

(b) For the purpose of this clause, the term "contractor" means the contractor, its subsidiaries and affiliates, joint ventures involving the contractor, any entity with which the contractor may hereafter merge or affiliate, and any other successor of the contractor.

(c) During the term of this contract and for a period of 1 year after completion of this contract, the Contractor agrees that it will not supply (whether as a prime contractor, subcontractor at any tier, or consultant to a supplier) to the Department of Defense, any product, item or major component of an item or product, which was the subject of the systems engineering and/or technical direction in support of Networks and Communications Division (Code 551) engineering support performed under this contract. The contractor shall, within 15 days after the effective date of this contract, provide, in writing, to the Contracting Officer, a representation that all employees, agents and subcontractors involved in the performance of this contract have been informed of the provisions of this clause. Any subcontractor that performs any work relative to this contract shall be subject to this clause. The contractor agrees to place in each subcontract affected by these provisions the necessary language contained in this clause.

(d) The Contractor further agrees that it will not perform engineering services and technical support of the type described in the SOW for any product it has designed, developed, or manufactured in whole or in part. The Contractor further agrees to notify the Contracting Officer should it be tasked to conduct engineering and technical support on such products and to take no action until directed to do so by the Contracting Officer.

(e) The Contractor acknowledges the full force and effect of this clause. It agrees to be bound by its terms and conditions and understands that violation of this clause may, in the judgment of the Contracting Officer, be cause for Termination for Default under FAR 52.249-6. The Contractor also acknowledges that this does not represent the sole and exclusive remedy available to the Government in the event the Contractor breaches this Organizational Conflict of Interest clause.

(End of clause)

5252.209-9202 ORGANIZATIONAL CONFLICT OF INTEREST (SPECIFICATION PREPARATION) (DEC 1999)

(a) This contract, in whole or in part, provides for the Contractor to draft and/or furnish specifications in support of Networks and Communications Division (Code 551) engineering support. Further, this contract may task the Contractor to prepare or assist in preparing work statements that directly, predictably and without delay are used in future competitive acquisitions in support of Networks and Communications Division (Code 551) engineering support. The parties recognize that by the Contractor providing this support a potential conflict of interest arises as defined by FAR 9.505-2.

(b) During the term of this contract and for a period of three years after completion of this contract, the Contractor agrees that it will not supply as a prime contractor, subcontractor at any tier, or consultant to a supplier to the Department of Defense, any product, item or major component of an item or product, which was the subject of the specifications and/or work statements furnished under this contract. The contractor shall, within 15 days after the effective date of this contract, provide, in writing, to the Contracting Officer, a representation that all employees, agents and subcontractors involved in the performance of this contract have been informed of the provisions of this clause. Any subcontractor that performs any work relative to this contract shall be subject to this clause. The contractor agrees to place in each subcontract affected by these provisions the necessary language contained in this clause.

(c) For the purposes of this clause, the term “contractor” means the contractor, its subsidiaries and affiliates, joint ventures involving the contractor, any entity with which the contractor may hereafter merge or affiliate and any other successor or assignee of the contractor.

(d) The Contractor acknowledges the full force and effect of this clause. It agrees to be bound by its terms and conditions and understands that violation of this clause may, in the judgment of the Contracting Officer, be cause for Termination for Default under FAR 52.249-6. The Contractor also acknowledges that this does not represent the sole and exclusive remedy available to the Government in the event the Contractor breaches this or any other Organizational Conflict of Interest clause.

(End of clause)

5252.209-9203 ORGANIZATIONAL CONFLICT OF INTEREST (ACCESS TO PROPRIETARY INFORMATION) (DEC 1999)

(a) This contract provides for the Contractor to provide technical evaluation and/or advisory and assistance services in support of Networks and Communications Division (Code 551) engineering support described in the PWS. The parties recognize that by the Contractor providing this support a potential conflict of interest arises as described by FAR 9.505-3 and FAR 9.505-4.

(b) For the purpose of this clause, the term “contractor” means the contractor, its subsidiaries and affiliates, joint ventures involving the contractor, any entity with which the contractor may hereafter merge or affiliate, and any other successor or assignee of the contractor.

(c) The Contractor agrees to execute agreements with companies furnishing proprietary data in connection with work performed under this contract, which obligates the Contractor to protect such data from unauthorized use or disclosure so long as such data remains proprietary, and to furnish copies of such agreements to the Contracting Officer. The Contractor further agrees that such proprietary data shall not be used in performing additional work for the Department of Defense in the same field as work performed under this contract whether as a prime, consultant or subcontractor at any tier.

(d) The contractor shall, within 15 days after the effective date of this contract, provide, in writing, to the Contracting Officer, a representation that all employees, agents and subcontractors involved in the performance of this contract have been informed of the provisions of this clause. Any subcontractor that performs any work relative to this contract shall be subject to this clause. The contractor agrees to place in each subcontract affected by these provisions the necessary language contained in this clause.

(e) The Contractor further agrees that it will not perform technical evaluations as described in the SOW for any product it has designed, developed, or manufactured in whole or in part. The Contractor further agrees to notify the Contracting Officer should it be tasked to conduct such technical evaluations on such products and to take no action unless directed to do so by the Contracting Officer.

(f) The Contractor acknowledges the full force and effect of this clause. It agrees to be bound by its terms and conditions and understands that violation of this clause may, in the judgment of the Contracting Officer, be cause for Termination for Default under FAR 52.249-6. The Contractor also acknowledges that this does not represent the sole and exclusive remedy available to the government in the event the Contractor breaches this or any other Organizational Conflict of Interest clause.

(End of clause)

5252.209-9204 EXISTING ORGANIZATIONAL CONFLICT OF INTEREST (FEB 1999)

(a) Definitions.

(1) "Contractor" means the firm signing this contract.

(2) "Supplier" means a firm, or a firm's subsidiaries, its parent corporation or subsidiary of the parent corporation, that is engaged in, or having a known prospective interest in the furnishing of Networks and Communications Division (Code 551) engineering support in support of which, tasks will be performed under this contract.

(3) "Affiliates" means employees, directors, partners, participants in joint ventures, parent corporation, parent corporation subsidiaries, any entity into or with which the contractor may subsequently merge or affiliate, any other successor or assignee of the prime contractor and subcontractors.

(4) "Interest" means direct or indirect business or financial interest.

(b) Warranty Against Existing Conflict of Interest. The contractor warrants that neither it nor its affiliates have any contracts with, or any material or substantial interests in the hardware or software suppliers. For any breach of this warranty, the Government shall have the right to rescind this contract without liability or, at its discretion, terminate this contract for default. In such circumstances, the contractor shall not be entitled to reimbursement of any cost incurred in performing this contract or payment of any fee thereunder. Further, such shall not be allocable or chargeable, directly or indirectly, to any other contract with the Government.

(End of clause)

5252.209-9205 ORGANIZATIONAL CONFLICT OF INTEREST (DEC 2004)

(a) Definition.

"Support Services" includes, but is not limited to, program management support services, preparing program budget submissions, business financial reporting or accounting services or, advisory and assistance services including consultant services

(b) The Contracting Officer has determined that potentially significant organizational conflicts of interest may arise due to the nature of the work the Contractor will perform under this contract that may preclude the Contractor from being awarded future SPAWAR contracts in a related area. Whereas the Contractor has agreed to undertake this contract to provide “support services”, it is agreed that the Contractor shall be ineligible to act as a prime contractor, consultant, or subcontractor to any prime contractor or subcontractor at any tier who is to supply the services, system or major components thereof for any project where the Contractor has provided or is providing support as described in FAR 9.505-1 through 9.505-4. The Contracting Officer may make a determination to allow a company to participate in an acquisition subject to the submission of an acceptable mitigation plan in accordance with paragraph (d) and (e) below. This determination may not be appealed.

(c) (1) If the Contracting Officer requests, and the Contractor submits an organizational conflict of interest mitigation plan that, after Government review is acceptable to the Government, the Contractor’s parent corporation, subsidiaries, or other physically separate profit and loss centers may not be precluded from acting as a subcontractor or consultant on future SPAWAR contracts. The Government’s determination regarding the adequacy of the mitigation plan or the possibility of mitigation are unilateral decisions made solely at the discretion of the Government and are not subject to the Disputes clause of the contract. The Government may terminate the contract for default if the Contractor fails to implement and follow the procedures contained in any approved mitigation plan.

(2) Any mitigation plan shall include, at a minimum, non-disclosure agreements to be executed by the Contractor and the Contractor’s employees supporting the Government per paragraph (c) above. Items for consideration in a mitigation plan include the following: identification of the organizational conflict(s) of interest; reporting and tracking system; an organizational conflict of interest compliance/enforcement plan, to include employee training and sanctions, in the event of unauthorized disclosure of sensitive information; a plan for organizational segregation (e.g., separate reporting chains); and data security measures.

(d) These restrictions shall apply to Scientific Research Corporation. This clause shall remain in effect for one year after completion of this contract.

(e) The Contractor shall apply this clause to any subcontractors or consultants, who have access to information, participate in the development of data, or participate in any other activity related to this contract which is subject to terms of this clause at the prime contractor level, unless the Contractor includes an acceptable alternate subcontractor provision in its mitigation plan. For subcontractors or consultants under this contract, if an organizational conflict of interest mitigation plan is submitted and acceptable to the Government, the subcontractor’s parent corporation, subsidiaries, or other physically separate profit and loss centers may not be precluded from acting as a prime, subcontractor, or consultant on future SPAWAR contracts.

5252.209-9206 EMPLOYMENT OF NAVY PERSONNEL RESTRICTED (DEC 1999)

In performing this contract, the Contractor will not use as a consultant or employ (on either a full or part-time basis) any active duty Navy personnel (civilian or military) without the prior approval of the Contracting Officer. Such approval may be given only in circumstances where it is clear that no law and no DOD or Navy instructions, regulations, or policies might possibly be contravened and no appearance of a conflict of interest will result.

(End of clause)

5252.216-9213 TYPES OF TASK OR DELIVERY ORDERS (DEC 1999)

The following types of task or delivery orders may be issued under this contract:

(*) A cost-plus-fixed-fee (CPFF) level of effort (LOE) task order will be issued when the scope of work is defined in general terms requiring only that the contractor devote a specified LOE for a stated time period.

(*) A cost-plus-fixed-fee (CPFF) completion task order will be issued when the scope of work defines a definite goal or target which leads to an end product deliverable (e.g., a final report of research accomplishing the goal or target).

(End of clause)

5252.217-9201 CONTRACT MAXIMUM AMOUNT (DEC 1999)

During the life of this contract, the total maximum dollar amount available for placement under task orders is cumulative with each option exercise, and unexpended balances may be used in succeeding option years.

(End of clause)

5252.219-9201 SMALL BUSINESS SUBCONTRACTING PLAN (OCT 2003)

Pursuant to Public Law 95-507, the Contractor's Subcontracting Plan for small business, HUBZone small business, small disadvantaged business, women-owned small business, veteran-owned small business, and service-disabled veteran-owned small business concerns is hereby approved and attached hereto as Attachment 2 and is made a part of this contract.

(End of clause)

5252.227-9206 SUBMISSION OF INTERIM AND FINAL INVENTION REPORTS AND NOTIFICATION OF ALL SUBCONTRACTS FOR EXPERIMENTAL, DEVELOPMENTAL, OR RESEARCH WORK (OCT 2008)

(a) This contract contains either FAR 52.227-11 "Patent Rights--Ownership by the Contractor" clause and DFARS 252.227-7039 "Patents--Reporting of Subject Inventions" or DFARS 252.227-7038 "Patent Rights--Ownership by the Contractor (Large Business)" clause, or FAR 52.227-13 "Patent Rights--Ownership by the Government" clause.

(b) Under these clauses, the Contractor is required to submit interim and final invention reports and notification to the Government of all subcontracts for experimental, developmental, or research work. The interim and final invention reports and notification of all subcontracts for experimental, developmental, or research work may be submitted on DD Form 882 "Report of Inventions and Subcontracts."

(c) The Contractor shall submit interim and final invention reports and notification of all subcontracts for experimental, developmental, or research work, including negative reports, to:

For contracts with SPAWARSYSCEN-Pacific, use:
CONTRACT CLOSEOUT / CODE 23200
SPAWARSYSCEN PACIFIC
53560 HULL STREET
SAN DIEGO, CA 92152-5001

SSC_PAC_Closeout@navy.mil

(d) The *SPAWARSYSCEN Pacific Office of Patent Counsel, Code 360012*, will represent the Contracting Officer with regard to invention reporting matters arising under the contract.

(End of clause)

5252.227-9207 LIMITED RELEASE OF CONTRACTOR CONFIDENTIAL BUSINESS INFORMATION (APRIL 2010)

(a) Definition.

“Confidential Business Information,” (Information) as used in this clause, is defined as all forms and types of financial, business, economic or other types of information other than technical data or computer software/computer software documentation, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if -- (1) the owner thereof has taken reasonable measures to keep such Information secret, and (2) the Information derives independent economic value, actual or potential from not being generally known to, and not being readily ascertainable through proper means by, the public. Information does not include technical data, as that term is defined in DFARS 252.227-7013(a)(14), 252.227-7015(a)(4), and 252.227-7018(a)(19). Similarly, Information does not include computer software/computer software documentation, as those terms are defined in DFARS 252.227-7014(a)(4) and 252.227-7018(a)(4).

(b) The Space and Naval Warfare Systems Command (SPAWAR) may release to individuals employed by SPAWAR support contractors and their subcontractors Information submitted by the contractor or its subcontractors pursuant to the provisions of this contract. Information that would ordinarily be entitled to confidential treatment may be included in the Information released to these individuals. Accordingly, by submission of a proposal or execution of this contract, the offeror or contractor and its subcontractors consent to a limited release of its Information, but only for purposes as described in paragraph (c) of this clause.

(c) Circumstances where SPAWAR may release the contractor’s or subcontractors’ Information include the following:

- (1) To other SPAWAR contractors and subcontractors, and their employees tasked with assisting SPAWAR in handling and processing Information and documents in the administration of SPAWAR contracts, such as file room management and contract closeout; and,
- (2) To SPAWAR contractors and subcontractors, and their employees tasked with assisting SPAWAR in accounting support services, including access to cost-reimbursement vouchers.

(d) SPAWAR recognizes its obligation to protect the contractor and its subcontractors from competitive harm that could result from the release of such Information. SPAWAR will permit the limited release of Information under paragraphs (c)(1) and (c)(2) only under the following conditions:

- (1) SPAWAR determines that access is required by other SPAWAR contractors and their subcontractors to perform the tasks described in paragraphs (c)(1) and (c)(2);
- (2) Access to Information is restricted to individuals with a bona fide need to possess;
- (3) Contractors and their subcontractors having access to Information have agreed under their contract or a separate corporate non-disclosure agreement to provide the same level of protection to the Information that would be provided by SPAWAR employees. Such contract terms or separate corporate non-disclosure agreement shall require the contractors and subcontractors to train their employees on how to properly handle the Information to which they will have access, and to have their employees sign company non disclosure agreements certifying that they understand the sensitive nature of the Information and that unauthorized use of the Information could expose their company to significant liability. Copies of such employee non disclosure agreements shall be provided to the Government;
- (4) SPAWAR contractors and their subcontractors performing the tasks described in paragraphs (c)(1) or (c)(2) have agreed under their contract or a separate non-disclosure agreement to not use the Information for any purpose other than performing the tasks described in paragraphs (c)(1) and (c)(2); and,

(5) Before releasing the Information to a non-Government person to perform the tasks described in paragraphs (c)(1) and (c)(2), SPAWAR shall provide the contractor a list of the company names to which access is being granted, along with a Point of Contact for those entities.

(e) SPAWAR's responsibilities under the Freedom of Information Act are not affected by this clause.

(f) The contractor agrees to include, and require inclusion of, this clause in all subcontracts at any tier that requires the furnishing of Information.

(End of clause)

5252.231-9200 REIMBURSEMENT OF TRAVEL COSTS (JAN 2006)

(a) Contractor Request and Government Approval of Travel

Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is a definite or indefinite delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract is not a definite or indefinite delivery contract, then the written Government authorization will be by written notice of approval from the Contracting Officer's Representative (COR). The request shall include as a minimum, the following:

- (1) Contract number
- (2) Date, time, and place of proposed travel
- (3) Purpose of travel and how it relates to the contract
- (4) Contractor's estimated cost of travel
- (5) Name(s) of individual(s) traveling and;
- (6) A breakdown of estimated travel and per diem charges.

Any travel under the contract must be specifically identified by the contractor in a written quotation to the Ordering Officer prior to incurring any travel costs. Travel under this contract is only authorized under task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order.

(b) General

(1) The costs for travel, subsistence, and lodging shall be reimbursed to the contractor only to the extent that it is necessary and authorized for performance of the work under this contract. The costs for travel, subsistence, and lodging shall be reimbursed to the contractor in accordance with the Federal Acquisition Regulation (FAR) 31.205-46, which is incorporated by reference into this contract. As specified in FAR 31.205-46(a) (2), reimbursement for the costs incurred for lodging, meals and incidental expenses (as defined in the travel regulations cited subparagraphs (b)(1)(i) through (b)(1)(iii) below) shall be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the following:

(i) Federal Travel Regulation prescribed by the General Services Administration for travel in the contiguous 48 United States;

(ii) Joint Travel Regulation, Volume 2, DoD Civilian Personnel, Appendix A, prescribed by the Department of Defense for travel in Alaska, Hawaii, The Commonwealth of Puerto Rico, and the territories and possessions of the United States; or

(iii) Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in the travel regulations cited in subparagraphs (b)(1)(i) and (b)(1)(ii) above.

(2) Personnel in travel status from and to the contractor's place of business and designated work site or vice versa, shall be considered to be performing work under the contract, and contractor shall bill such travel time at the straight (regular) time rate; however, such billing shall not exceed eight hours per person for any one person while in travel status during one calendar day.

(c) Per Diem

(1) The contractor shall not be paid per diem for contractor personnel who reside in the metropolitan area in which the tasks are being performed. Per diem shall not be paid on services performed at contractor's home facility and at any facility required by the contract, or at any location within a radius of 50 miles from the contractor's home facility and any facility required by this contract.

(2) Costs for subsistence and lodging shall be paid to the contractor only to the extent that overnight stay is necessary and authorized in writing by the Government for performance of the work under this contract per paragraph (a). When authorized, per diem shall be paid by the contractor to its employees at a rate not to exceed the rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and authorized in writing by the Government. The authorized per diem rate shall be the same as the prevailing locality per diem rate.

(3) Reimbursement to the contractor for per diem shall be limited to payments to employees not to exceed the authorized per diem and as authorized in writing by the Government per paragraph (a). Fractional parts of a day shall be payable on a prorated basis for purposes of billing for per diem charges attributed to subsistence on days of travel. The departure day from the Permanent Duty Station (PDS) and return day to the PDS shall be 75% of the applicable per diem rate. The contractor shall retain supporting documentation for per diem paid to employees as evidence of actual payments, as required by the FAR 52.216-7 "Allowable Cost and Payment" clause of the contract.

(d) Transportation

(1) The contractor shall be paid on the basis of actual amounts paid to the extent that such transportation is necessary for the performance of work under the contract and is authorized in writing by the Government per paragraph (a).

(2) The contractor agrees, in the performance of necessary travel, to use the lowest cost mode commensurate with the requirements of the mission and in accordance with good traffic management principles. When it is necessary to use air or rail travel, the contractor agrees to use coach, tourist class or similar accommodations to the extent consistent with the successful and economical accomplishment of the mission for which the travel is being performed. Documentation must be provided to substantiate non-availability of coach or tourist if business or first class is proposed to accomplish travel requirements.

(3) When transportation by privately owned conveyance (POC) is authorized, the contractor shall be paid on a mileage basis not to exceed the applicable Government transportation rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and is authorized in writing by the Government per paragraph (a).

(4) When transportation by privately owned (motor) vehicle (POV) is authorized, required travel of contractor personnel, that is not commuting travel, may be paid to the extent that it exceeds the normal commuting mileage of such employee. When an employee's POV is used for travel between an employee's residence or the Permanent Duty Station and one or more alternate work sites within the local area, the employee shall be paid mileage for the distance that exceeds the employee's commuting distance.

(5) When transportation by a rental automobile, other special conveyance or public conveyance is authorized, the contractor shall be paid the rental and/or hiring charge and operating expenses incurred on official

business (if not included in the rental or hiring charge). When the operating expenses are included in the rental or hiring charge, there should be a record of those expenses available to submit with the receipt. Examples of such operating expenses include: hiring charge (bus, streetcar or subway fares), gasoline and oil, parking, and tunnel tolls.

(6) Definitions:

(i) “Permanent Duty Station” (PDS) is the location of the employee’s permanent work assignment (i.e., the building or other place where the employee regularly reports for work).

(ii) “Privately Owned Conveyance” (POC) is any transportation mode used for the movement of persons from place to place, other than a Government conveyance or common carrier, including a conveyance loaned for a charge to, or rented at personal expense by, an employee for transportation while on travel when such rental conveyance has not been authorized/approved as a Special Conveyance.

(iii) “Privately Owned (Motor) Vehicle (POV)” is any motor vehicle (including an automobile, light truck, van or pickup truck) owned by, or on a long-term lease (12 or more months) to, an employee or that employee’s dependent for the primary purpose of providing personal transportation, that:

- (a) is self-propelled and licensed to travel on the public highways;
- (b) is designed to carry passengers or goods; and
- (c) has four or more wheels or is a motorcycle or moped.

(iv) “Special Conveyance” is commercially rented or hired vehicles other than a POC and other than those owned or under contract to an agency.

(v) “Public Conveyance” is local public transportation (e.g., bus, streetcar, subway, etc) or taxicab.

(iv) “Residence” is the fixed or permanent domicile of a person that can be reasonably justified as a bona fide residence.

EXAMPLE 1: Employee’s one way commuting distance to regular place of work is 7 miles. Employee drives from residence to an alternate work site, a distance of 18 miles. Upon completion of work, employee returns to residence, a distance of 18 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (14 miles). The employee is reimbursed for 22 miles ($18 + 18 - 14 = 22$).

EXAMPLE 2: Employee’s one way commuting distance to regular place of work is 15 miles. Employee drives from residence to an alternate work site, a distance of 5 miles. Upon completion of work, employee returns to residence, a distance of 5 miles.

In this case, the employee is not entitled to be reimbursed for the travel performed (10 miles), since the distance traveled is less than the commuting distance (30 miles) to the regular place of work.

EXAMPLE 3: Employee’s one way commuting distance to regular place of work is 15 miles. Employee drives to regular place of work. Employee is required to travel to an alternate work site, a distance of 30 miles. Upon completion of work, employee returns to residence, a distance of 15 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (30 miles). The employee is reimbursed for 30 miles ($15 + 30 + 15 - 30 = 30$).

EXAMPLE 4: Employee's one way commuting distance to regular place of work is 12 miles. In the morning the employee drives to an alternate work site (45 miles). In the afternoon the employee returns to the regular place of work (67 miles). After completion of work, employee returns to residence, a distance of 12 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (24 miles). The employee is reimbursed for 100 miles ($45 + 67 + 12 - 24 = 100$).

EXAMPLE 5: Employee's one way commuting distance to regular place of work is 35 miles. Employee drives to the regular place of work (35 miles). Later, the employee drives to alternate work site #1 (50 miles) and then to alternate work site #2 (25 miles). Employee then drives to residence (10 miles).

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal commuting distance (70 miles). The employee is reimbursed for 50 miles ($35 + 50 + 25 + 10 - 70 = 50$).

EXAMPLE 6: Employee's one way commuting distance to regular place of work is 20 miles. Employee drives to the regular place of work (20 miles). Later, the employee drives to alternate work site #1 (10 miles) and then to alternate work site #2 (5 miles). Employee then drives to residence (2 miles).

In this case, the employee is not entitled to be reimbursed for the travel performed (37 miles), since the distance traveled is less than the commuting distance (40 miles) to the regular place of work.

5252.237-9602 CONTRACTOR IDENTIFICATION (MAY 2004)

- (a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.
- (b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.
- (c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with Contractor supplied signs, name plates or other identification, showing that these are work areas for Contractor or subcontractor personnel.

(End of clause)

5252.237-9603 REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION (AUG 2011)

- (a) Definition. As used in this clause, "sensitive information" includes:
 - (i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
 - (ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);

- (iii) Information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;
- (iv) Other information designated as sensitive by the Space and Naval Warfare Systems Command (SPAWAR).

(b) In the performance of the contract, the Contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements.

(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The Contractor shall—

- (i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;
- (ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;
- (iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contract and to safeguard information from unauthorized use and disclosure.
- (iv) Execute a “Contractor Access to Information Non-Disclosure Agreement,” and obtain and submit to the Contracting Officer a signed “Contractor Employee Access to Information Non-Disclosure Agreement” for each employee prior to assignment;
- (v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the Contractor inadvertently accesses or receives any information marked as “proprietary,” “procurement sensitive,” or “source selection sensitive,” or that, even if not properly marked otherwise indicates the Contractor may not be authorized to access such information, the Contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this clause are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government Information Systems.

(f) Subcontracts. The Contractor shall insert paragraphs (a) through (f) of this clause in all subcontracts that may require access to sensitive information in the performance of the contract.

(g) Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the “Contractor Non-Disclosure Agreement,” a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the Contractor’s plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate Contractor personnel requiring access to information in the

performance of the contract from other Contractor personnel to ensure that the Contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A “firewall” may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The Contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

(End of clause)

5252.243-9600 AUTHORIZED CHANGES ONLY BY THE CONTRACTING OFFICER (JAN 1992)

(a) Except as specified in paragraph (b) below, no order, statement, or conduct of Government personnel who visit the Contractor’s facilities or in any other manner communicates with Contractor personnel during the performance of this contract shall constitute a change under the Changes clause of this contract.

(b) The Contractor shall not comply with any order, direction or request of Government personnel unless it is issued in writing and signed by the Contracting Officer, or is pursuant to specific authority otherwise included as a part of this contract.

(c) The Contracting Officer is the only person authorized to approve changes in any of the requirements of this contract and notwithstanding provisions contained elsewhere in this contract, the said authority remains solely the Contracting Officer’s. In the event the contractor effects any change at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in charges incurred as a result thereof. The Contracting Officer is:

Any warranted Contracting Officer at SPAWAR Systems Center Pacific

(End of clause)

Section I - Contract Clauses

CLAUSES INCORPORATED BY REFERENCE

52.202-1	Definitions	JAN 2012
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	APR 1984
52.203-6	Restrictions On Subcontractor Sales To The Government	SEP 2006
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	JAN 1997
52.203-10	Price Or Fee Adjustment For Illegal Or Improper Activity	JAN 1997
52.203-12	Limitation On Payments To Influence Certain Federal Transactions	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct	APR 2010
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUL 2013
52.204-13	System for Award Management Maintenance	JUL 2013
52.204-15	Service Contract Reporting Requirements for Indefinite-Delivery Contracts	JAN 2014
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	AUG 2013
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013
52.209-10	Prohibition on Contracting With Inverted Domestic Corporations	DEC 2014
52.215-2	Audit and Records--Negotiation	OCT 2010
52.215-8	Order of Precedence--Uniform Contract Format	OCT 1997
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data--Modifications	AUG 2011
52.215-13	Subcontractor Certified Cost or Pricing Data--Modifications	OCT 2010
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other than Pensions	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Certified Cost or Pricing Data or Information Other Than Certified Cost or Pricing Data--Modifications	OCT 2010
52.215-21 Alt III	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data -- Modifications (Oct 2010) - Alternate III	OCT 1997
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost And Payment	JUN 2013
52.216-8	Fixed Fee	JUN 2011
52.219-8	Utilization of Small Business Concerns	OCT 2014
52.219-9	Small Business Subcontracting Plan	OCT 2014

52.219-9 (Dev)	Small Business Subcontracting Plan (Deviation 2013-O0014)	OCT 2014
52.219-9 Alt II	Small Business Subcontracting Plan (OCT 2014) Alternate II	OCT 2001
52.219-16	Liquidated Damages-Subcontracting Plan	JAN 1999
52.219-28	Post-Award Small Business Program Rerepresentation	JUL 2013
52.222-3	Convict Labor	JUN 2003
52.222-21	Prohibition Of Segregated Facilities	FEB 1999
52.222-26	Equal Opportunity	MAR 2007
52.222-35	Equal Opportunity for Veterans	JUL 2014
52.222-36	Equal Opportunity for Workers with Disabilities	JUL 2014
52.222-37	Employment Reports on Veterans	JUL 2014
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
52.222-50	Combating Trafficking in Persons	MAR 2015
52.222-54	Employment Eligibility Verification	AUG 2013
52.222-99 (Dev)	Establishing a Minimum Wage for Contractors (Deviation 2014-O0017)	JUN 2014
52.223-5	Pollution Prevention and Right-to-Know Information	MAY 2011
52.223-6	Drug-Free Workplace	MAY 2001
52.223-10	Waste Reduction Program	MAY 2011
52.223-15	Energy Efficiency in Energy-Consuming Products	DEC 2007
52.223-16	Acquisition of EPEAT -Registered Personal Computer Products	JUN 2014
52.223-17	Affirmative Procurement of EPA-Designated Items in Service and Construction Contracts	MAY 2008
52.223-18	Encouraging Contractor Policies To Ban Text Messaging While Driving	AUG 2011
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.227-1	Authorization and Consent	DEC 2007
52.227-1 Alt I	Authorization And Consent (Dec 2007) - Alternate I	APR 1984
52.227-2	Notice And Assistance Regarding Patent And Copyright Infringement	DEC 2007
52.227-3	Patent Indemnity	APR 1984
52.227-10	Filing Of Patent Applications--Classified Subject Matter	DEC 2007
52.227-11	Patent Rights--Ownership By The Contractor	MAY 2014
52.228-3	Worker's Compensation Insurance (Defense Base Act)	JUL 2014
52.228-7	Insurance--Liability To Third Persons	MAR 1996
52.230-2	Cost Accounting Standards	MAY 2014
52.230-3	Disclosure And Consistency Of Cost Accounting Practices	MAY 2014
52.230-6	Administration of Cost Accounting Standards	JUN 2010
52.232-9	Limitation On Withholding Of Payments	APR 1984
52.232-17	Interest	MAY 2014
52.232-20	Limitation Of Cost	APR 1984
52.232-22	Limitation Of Funds	APR 1984
52.232-23	Assignment Of Claims	MAY 2014
52.232-25	Prompt Payment	JUL 2013
52.232-25 Alt I	Prompt Payment (July 2013) Alternate I	FEB 2002
52.232-33	Payment by Electronic Funds Transfer--System for Award Management	JUL 2013
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.233-1	Disputes	MAY 2014
52.233-1 Alt I	Disputes (May 2014) - Alternate I	DEC 1991
52.233-3	Protest After Award	AUG 1996

52.233-3 Alt I	Protest After Award (Aug 1996) - Alternate I	JUN 1985
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-2	Protection Of Government Buildings, Equipment, And Vegetation	APR 1984
52.237-3	Continuity Of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.242-1	Notice of Intent to Disallow Costs	APR 1984
52.242-3	Penalties for Unallowable Costs	MAY 2014
52.242-4	Certification of Final Indirect Costs	JAN 1997
52.242-13	Bankruptcy	JUL 1995
52.243-2	Changes--Cost-Reimbursement	AUG 1987
52.243-2 Alt V	Changes--Cost-Reimbursement (Aug 1987) - Alternate V	APR 1984
52.244-5	Competition In Subcontracting	DEC 1996
52.244-6	Subcontracts for Commercial Items	MAR 2015
52.245-1	Government Property	APR 2012
52.245-9	Use And Charges	APR 2012
52.246-25	Limitation Of Liability--Services	FEB 1997
52.247-1	Commercial Bill Of Lading Notations	FEB 2006
52.247-63	Preference For U.S. Flag Air Carriers	JUN 2003
52.248-1	Value Engineering	OCT 2010
52.249-6	Termination (Cost Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012
52.253-1	Computer Generated Forms	JAN 1991
252.201-7000	Contracting Officer's Representative	DEC 1991
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.203-7001	Prohibition On Persons Convicted of Fraud or Other Defense-Contract-Related Felonies	DEC 2008
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.203-7003	Agency Office of the Inspector General	DEC 2012
252.203-7004	Display of Fraud Hotline Poster(s)	JAN 2015
252.204-7000	Disclosure Of Information	AUG 2013
252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7005	Oral Attestation of Security Responsibilities	NOV 2001
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Country that is a State Sponsor of Terrorism	DEC 2014
252.211-7008	Use of Government-Assigned Serial Numbers	SEP 2010
252.215-7000	Pricing Adjustments	DEC 2012
252.216-7006	Ordering	MAY 2011
252.219-7003	Small Business Subcontracting Plan (DOD Contracts)	OCT 2014
252.222-7002	Compliance With Local Labor Laws (Overseas)	JUN 1997
252.222-7006	Restrictions on the Use of Mandatory Arbitration Agreements	DEC 2010
252.223-7004	Drug Free Work Force	SEP 1988
252.223-7006	Prohibition On Storage, Treatment, and Disposal of Toxic or Hazardous Materials	SEP 2014
252.225-7004	Report of Intended Performance Outside the United States and Canada--Submission after Award	OCT 2010
252.225-7012	Preference For Certain Domestic Commodities	FEB 2013
252.225-7041	Correspondence in English	JUN 1997
252.225-7043	Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States	MAR 2006
252.225-7048	Export-Controlled Items	JUN 2013

252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7013	Rights in Technical Data--Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.227-7015	Technical Data--Commercial Items	FEB 2014
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7019	Validation of Asserted Restrictions--Computer Software	SEP 2011
252.227-7025	Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends	MAY 2013
252.227-7027	Deferred Ordering Of Technical Data Or Computer Software	APR 1988
252.227-7030	Technical Data--Withholding Of Payment	MAR 2000
252.227-7037	Validation of Restrictive Markings on Technical Data	JUN 2013
252.227-7038	Patent Rights--Ownership by the Contractor (Large Business)	JUN 2012
252.227-7039	Patents--Reporting Of Subject Inventions	APR 1990
252.231-7000	Supplemental Cost Principles	DEC 1991
252.232-7003	Electronic Submission of Payment Requests and Receiving Reports	JUN 2012
252.232-7010	Levies on Contract Payments	DEC 2006
252.233-7001	Choice of Law (Overseas)	JUN 1997
252.235-7003	Frequency Authorization	MAR 2014
252.235-7011	Final Scientific or Technical Report	JAN 2015
252.237-7010	Prohibition on Interrogation of Detainees by Contractor Personnel	JUN 2013
252.242-7004	Material Management And Accounting System	MAY 2011
252.242-7005	Contractor Business Systems	FEB 2012
252.242-7006	Accounting System Administration	FEB 2012
252.244-7001	Contractor Purchasing System Administration	MAY 2014
252.245-7001	Tagging, Labeling, and Marking of Government-Furnished Property	APR 2012
252.245-7002	Reporting Loss of Government Property	APR 2012
252.245-7003	Contractor Property Management System Administration	APR 2012
252.246-7000	Material Inspection And Receiving Report	MAR 2008
252.246-7003	Notification of Potential Safety Issues	JUN 2013
252.246-7006	Warranty Tracking of Serialized Items	JUN 2011

CLAUSES INCORPORATED BY FULL TEXT

52.216-19 ORDER LIMITATIONS. (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than **\$2,500**, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor:

(1) Any order for a single item in excess of **the total balance of the contract ceiling**;

(2) Any order for a combination of items in excess of **the total balance of the contract ceiling**; or

(3) A series of orders from the same ordering office within **one (1)** day that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) above.

(d) Notwithstanding paragraphs (b) and (c) above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within one (1) day after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

52.216-22 INDEFINITE QUANTITY. (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum". The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum".

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after **all task orders issued during the ordering period have expired**.

(End of clause)

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of contract expiration.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within the ordering period of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to

extend at least thirty (30) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years.

(End of clause)

52.222-2 PAYMENT FOR OVERTIME PREMIUMS (JUL 1990)

(a) The use of overtime is authorized under this contract if the overtime premium cost does not exceed zero or the overtime premium is paid for work --

(1) Necessary to cope with emergencies such as those resulting from accidents, natural disasters, breakdowns of production equipment, or occasional production bottlenecks of a sporadic nature;

(2) By indirect-labor employees such as those performing duties in connection with administration, protection, transportation, maintenance, standby plant protection, operation of utilities, or accounting;

(3) To perform tests, industrial processes, laboratory procedures, loading or unloading of transportation conveyances, and operations in flight or afloat that are continuous in nature and cannot reasonably be interrupted or completed otherwise; or

(4) That will result in lower overall costs to the Government.

(b) Any request for estimated overtime premiums that exceeds the amount specified above shall include all estimated overtime for contract completion and shall--

(1) Identify the work unit; e.g., department or section in which the requested overtime will be used, together with present workload, staffing, and other data of the affected unit sufficient to permit the Contracting Officer to evaluate the necessity for the overtime;

(2) Demonstrate the effect that denial of the request will have on the contract delivery or performance schedule;

(3) Identify the extent to which approval of overtime would affect the performance or payments in connection with other Government contracts, together with identification of each affected contract; and

(4) Provide reasons why the required work cannot be performed by using multishift operations or by employing additional personnel.

* Insert either "zero" or the dollar amount agreed to during negotiations. The inserted figure does not apply to the exceptions in paragraph (a)(1) through (a)(4) of the clause.

(End of clause)

52.225-13 RESTRICTIONS ON CERTAIN FOREIGN PURCHASES (JUN 2008)

(a) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation,

Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(b) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas. Lists of entities and individuals subject to economic sanctions are included in OFAC's List of Specially Designated Nationals and Blocked Persons at [TerList1.html](http://www.treas.gov/offices/enforcement/ofac/). More information about these restrictions, as well as updates, is available in the OFAC's regulations at 31 CFR chapter V and/or on OFAC's Web site at <http://www.treas.gov/offices/enforcement/ofac/>.

(c) The Contractor shall insert this clause, including this paragraph (c), in all subcontracts.

(End of clause)

52.244-2 SUBCONTRACTS (OCT 2010)

(a) Definitions. As used in this clause--

Approved purchasing system means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).

Consent to subcontract means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

Subcontract means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that—

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds—

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

Notwithstanding the language contained in paragraph (c), written consent from the Contracting Officer is required prior to entering into any subcontract over the simplified acquisition threshold that was not initially proposed.

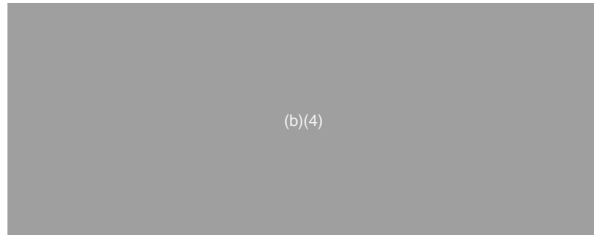
(e)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

- (i) A description of the supplies or services to be subcontracted.
- (ii) Identification of the type of subcontract to be used.
- (iii) Identification of the proposed subcontractor.
- (iv) The proposed subcontract price.
- (v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.
- (vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.
- (vii) A negotiation memorandum reflecting—
 - (A) The principal elements of the subcontract price negotiations;
 - (B) The most significant considerations controlling establishment of initial or revised prices;
 - (C) The reason certified cost or pricing data were or were not required;
 - (D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;
 - (E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;
 - (F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and
 - (G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.
- (2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (c), (d), or (e) of this clause.
- (f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination—
 - (1) Of the acceptability of any subcontract terms or conditions;
 - (2) Of the allowability of any cost under this contract; or
 - (3) To relieve the Contractor of any responsibility for performing this contract.
- (g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:



(End of clause)

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

<http://www.acquisition.gov/far/>
<http://farsite.hill.af.mil>

(End of clause)

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation Supplement (DFARS) (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (DEC 2013)

(a) Definitions. As used in this clause'

Automatic identification device means a device, such as a reader or interrogator, used to retrieve data encoded on machine-readable media.

Concatenated unique item identifier means--

(1) For items that are serialized within the enterprise identifier, the linking together of the unique identifier data elements in order of the issuing agency code, enterprise identifier, and unique serial number within the enterprise identifier; or

(2) For items that are serialized within the original part, lot, or batch number, the linking together of the unique identifier data elements in order of the issuing agency code; enterprise identifier; original part, lot, or batch number; and serial number within the original part, lot, or batch number.

Data Matrix means a two-dimensional matrix symbology, which is made up of square or, in some cases, round modules arranged within a perimeter finder pattern and uses the Error Checking and Correction 200 (ECC200) specification found within International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 16022.

Data qualifier means a specified character (or string of characters) that immediately precedes a data field that defines the general category or intended use of the data that follows.

DoD recognized unique identification equivalent means a unique identification method that is in commercial use and has been recognized by DoD. All DoD recognized unique identification equivalents are listed at http://www.acq.osd.mil/dpap/pdi/uid/iuid_equivalents.html.

DoD item unique identification means a system of marking items delivered to DoD with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items. For items that are serialized within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier and a unique serial number. For items that are serialized within the part, lot, or batch number within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier; the original part, lot, or batch number; and the serial number.

Enterprise means the entity (e.g., a manufacturer or vendor) responsible for assigning unique item identifiers to items.

Enterprise identifier means a code that is uniquely assigned to an enterprise by an issuing agency.

Government's unit acquisition cost means--

(1) For fixed-price type line, subline, or exhibit line items, the unit price identified in the contract at the time of delivery;

(2) For cost-type or undefinitized line, subline, or exhibit line items, the Contractor's estimated fully burdened unit cost to the Government at the time of delivery; and

(3) For items produced under a time-and-materials contract, the Contractor's estimated fully burdened unit cost to the Government at the time of delivery.

Issuing agency means an organization responsible for assigning a globally unique identifier to an enterprise (e.g., Dun & Bradstreet's Data Universal Numbering System (DUNS) Number, GS1 Company Prefix, Allied Committee 135 NATO Commercial and Government Entity (NCAGE)/Commercial and Government Entity (CAGE) Code, or the Coded Representation of the North American Telecommunications Industry Manufacturers, Suppliers, and Related Service Companies (ATIS-0322000) Number), European Health Industry Business Communication Council (EHIBCC) and Health Industry Business Communication Council (HIBCC)), as indicated in the Register of Issuing

Agency Codes for ISO/IEC 15459, located at <http://www.nen.nl/Normontwikkeling/Certificatieschemas-en-keurmerken/Schemabeheer/ISOIEC-15459.htm>.

Issuing agency code means a code that designates the registration (or controlling) authority for the enterprise identifier.

Item means a single hardware article or a single unit formed by a grouping of subassemblies, components, or constituent parts.

Lot or batch number means an identifying number assigned by the enterprise to a designated group of items, usually referred to as either a lot or a batch, all of which were manufactured under identical conditions.

Machine-readable means an automatic identification technology media, such as bar codes, contact memory buttons, radio frequency identification, or optical memory cards.

Original part number means a combination of numbers or letters assigned by the enterprise at item creation to a class of items with the same form, fit, function, and interface.

Parent item means the item assembly, intermediate component, or subassembly that has an embedded item with a unique item identifier or DoD recognized unique identification equivalent.

Serial number within the enterprise identifier means a combination of numbers, letters, or symbols assigned by the enterprise to an item that provides for the differentiation of that item from any other like and unlike item and is never used again within the enterprise.

Serial number within the part, lot, or batch number means a combination of numbers or letters assigned by the enterprise to an item that provides for the differentiation of that item from any other like item within a part, lot, or batch number assignment.

Serialization within the enterprise identifier means each item produced is assigned a serial number that is unique among all the tangible items produced by the enterprise and is never used again. The enterprise is responsible for ensuring unique serialization within the enterprise identifier.

Serialization within the part, lot, or batch number means each item of a particular part, lot, or batch number is assigned a unique serial number within that part, lot, or batch number assignment. The enterprise is responsible for ensuring unique serialization within the part, lot, or batch number within the enterprise identifier.

Type designation means a combination of letters and numerals assigned by the Government to a major end item, assembly or subassembly, as appropriate, to provide a convenient means of differentiating between items having the same basic name and to indicate modifications and changes thereto.

Unique item identifier means a set of data elements marked on items that is globally unique and unambiguous. The term includes a concatenated unique item identifier or a DoD recognized unique identification equivalent.

Unique item identifier type means a designator to indicate which method of uniquely identifying a part has been used. The current list of accepted unique item identifier types is maintained at http://www.acq.osd.mil/dpap/pdi/uid/uii_types.html.

(b) The Contractor shall deliver all items under a contract line, subline, or exhibit line item.

(c) Unique item identifier. (1) The Contractor shall provide a unique item identifier for the following:

(i) Delivered items for which the Government's unit acquisition cost is \$5,000 or more, except for the following line items:

Contract line, subline, or exhibit line item No.	Item description
.....	

(ii) Items for which the Government's unit acquisition cost is less than \$5,000 that are identified in the Schedule or the following table:

Contract line, subline, or exhibit line item No.	Item description
.....	

(If items are identified in the Schedule, insert "See Schedule" in this table.)

(iii) Subassemblies, components, and parts embedded within delivered items, items with warranty requirements, DoD serially managed reparable and DoD serially managed nonreparable as specified in Attachment Number ----.

(iv) Any item of special tooling or special test equipment as defined in FAR 2.101 that have been designated for preservation and storage for a Major Defense Acquisition Program as specified in Attachment Number ----.

(v) Any item not included in paragraphs (c)(1)(i), (ii), (iii), or

(iv) of this clause for which the contractor creates and marks a unique item identifier for traceability.

(2) The unique item identifier assignment and its component data element combination shall not be duplicated on any other item marked or registered in the DoD Item Unique Identification Registry by the contractor.

(3) The unique item identifier component data elements shall be marked on an item using two dimensional data matrix symbology that complies with ISO/IEC International Standard 16022, Information technology--International symbology specification--Data matrix; ECC200 data matrix specification.

(4) Data syntax and semantics of unique item identifiers. The Contractor shall ensure that--

(i) The data elements (except issuing agency code) of the unique item identifier are encoded within the data matrix symbol that is marked on the item using one of the following three types of data qualifiers, as determined by the Contractor:

(A) Application Identifiers (AIs) (Format Indicator 05 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology--EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(B) Data Identifiers (DIs) (Format Indicator 06 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology--EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(C) Text Element Identifiers (TEIs) (Format Indicator 12 of ISO/IEC International Standard 15434), in accordance with the Air Transport Association Common Support Data Dictionary; and

(ii) The encoded data elements of the unique item identifier conform to the transfer structure, syntax, and coding of messages and data formats specified for Format Indicators 05, 06, and 12 in ISO/IEC International Standard 15434, Information Technology-Transfer Syntax for High Capacity Automatic Data Capture Media.

(5) Unique item identifier.

(i) The Contractor shall--

(A) Determine whether to--

(1) Serialize within the enterprise identifier;

(2) Serialize within the part, lot, or batch number; or

(3) Use a DoD recognized unique identification equivalent (e.g. Vehicle Identification Number); and

(B) Place the data elements of the unique item identifier (enterprise identifier; serial number; DoD recognized unique identification equivalent; and for serialization within the part, lot, or batch number only: Original part, lot, or batch number) on items requiring marking by paragraph (c)(1) of this clause, based on the criteria provided in MIL-STD-130, Identification Marking of U.S. Military Property, latest version;

(C) Label shipments, storage containers and packages that contain uniquely identified items in accordance with the requirements of MIL-STD-129, Military Marking for Shipment and Storage, latest version; and

(D) Verify that the marks on items and labels on shipments, storage containers, and packages are machine readable and conform to the applicable standards. The contractor shall use an automatic identification technology device for this verification that has been programmed to the requirements of Appendix A, MIL-STD-130, latest version.

(ii) The issuing agency code--

(A) Shall not be placed on the item; and

(B) Shall be derived from the data qualifier for the enterprise identifier.

(d) For each item that requires item unique identification under paragraph (c)(1)(i), (ii), or (iv) of this clause or when item unique identification is provided under paragraph (c)(1)(v), in addition to the information provided as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the Contractor shall report at the time of delivery, as part of the Material Inspection and Receiving Report, the following information:

(1) Unique item identifier.

(2) Unique item identifier type.

(3) Issuing agency code (if concatenated unique item identifier is used).

(4) Enterprise identifier (if concatenated unique item identifier is used).

(5) Original part number (if there is serialization within the original part number).

(6) Lot or batch number (if there is serialization within the lot or batch number).

(7) Current part number (optional and only if not the same as the original part number).

(8) Current part number effective date (optional and only if current part number is used).

(9) Serial number (if concatenated unique item identifier is used).

(10) Government's unit acquisition cost.

(11) Unit of measure.

(e) For embedded subassemblies, components, and parts that require DoD unique item identification under paragraph (c)(1)(iii) of this clause, the Contractor shall report as part of, or associated with, the Material Inspection and Receiving Report specified elsewhere in this contract, the following information:

(1) Unique item identifier of the parent item under paragraph (c)(1) of this clause that contains the embedded subassembly, component, or part.

(2) Unique item identifier of the embedded subassembly, component, or part.

(3) Unique item identifier type.**

(4) Issuing agency code (if concatenated unique item identifier is used).**

(5) Enterprise identifier (if concatenated unique item identifier is used).**

(6) Original part number (if there is serialization within the original part number).**

(7) Lot or batch number (if there is serialization within the lot or batch number).**

(8) Current part number (optional and only if not the same as the original part number).**

(9) Current part number effective date (optional and only if current part number is used).**

(10) Serial number (if concatenated unique item identifier is used).**

(11) Description.

(12) Type designation of the item as specified in the contract schedule, if any.

(13) Whether the item is an item of Special Tooling or Special Test Equipment.

(14) Whether the item is covered by a warranty.

** Once per item.

(e) For embedded subassemblies, components, and parts that require DoD item unique identification under paragraph (c)(1)(iii) of this clause or when item unique identification is provided under paragraph (c)(1)(v), the Contractor shall report as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the following information:

(f) The Contractor shall submit the information required by paragraphs (d) and (e) of this clause as follows:

(1) End items shall be reported using the receiving report capability in Wide Area WorkFlow (WAWF) in accordance with the clause at 252.232-7003. If WAWF is not required by this contract, and the contractor is not using WAWF, follow the procedures at <http://dodprocurementtoolbox.com/site/uidregistry/>.

(2) Embedded items shall be reported by one of the following methods--

- (i) Use of the embedded items capability in WAWF;
 - (ii) Direct data submission to the IUID Registry following the procedures and formats at <http://dodprocurementtoolbox.com/site/uidregistry/>; or
 - (iii) Via WAWF as a deliverable attachment for exhibit line item number (fill in) ----, Unique Item Identifier Report for Embedded Items, Contract Data Requirements List, DD Form 1423.
- (g) Subcontracts. If the Contractor acquires by contract any items for which item unique identification is required in accordance with paragraph (c)(1) of this clause, the Contractor shall include this clause, including this paragraph (g), in the applicable subcontract(s), including subcontracts for commercial items.
- (End of clause)

252.211-7007 REPORTING OF GOVERNMENT-FURNISHED PROPERTY (AUG 2012)

(a) Definitions. As used in this clause—

“Commercial and Government entity (CAGE) code” means—

- (i) A code assigned by the Defense Logistics Agency Logistics Information Service to identify a commercial or Government entity; or
- (ii) A code assigned by a member of the North Atlantic Treaty Organization that the Defense Logistics Agency Logistics Information Service records and maintains in the CAGE master file. The type of code is known as an “NCAGE code.”

“Contractor-acquired property” has the meaning given in FAR clause 52.245-1. Upon acceptance by the Government, contractor-acquired property becomes Government-furnished property.

“Government-furnished property” has the meaning given in FAR clause 52.245-1.

“Item unique identification (IUID)” means a system of assigning, reporting, and marking DoD property with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items.

“IUID Registry” means the DoD data repository that receives input from both industry and Government sources and provides storage of, and access to, data that identifies and describes tangible Government personal property. The IUID Registry is—

- (i) The authoritative source of Government unit acquisition cost for items with unique item identification (see DFARS 252.211-7003) that were acquired after January 1, 2004;
- (ii) The master data source for Government-furnished property; and
- (iii) An authoritative source for establishing the acquisition cost of end-item equipment.

“National stock number (NSN)” means a 13-digit stock number used to identify items of supply. It consists of a four-digit Federal Supply Code and a nine-digit National Item Identification Number.

“Nomenclature” means—

- (i) The combination of a Government-assigned type designation and an approved item name;
- (ii) Names assigned to kinds and groups of products; or
- (iii) Formal designations assigned to products by customer or supplier (such as model number or model type, design differentiation, or specific design series or configuration).

“Part or identifying number (PIN)” means the identifier assigned by the original design activity, or by the controlling nationally recognized standard, that uniquely identifies (relative to that design activity) a specific item.

“Reparable” means an item, typically in unserviceable condition, furnished to the Contractor for maintenance, repair, modification, or overhaul.

“Serially managed item” means an item designated by DoD to be uniquely tracked, controlled, or managed in maintenance, repair, and/or supply systems by means of its serial number.

“Supply condition code” means a classification of materiel in terms of readiness for issue and use or to identify action underway to change the status of materiel

(see <http://www2.dla.mil/j-6/dlmsso/elibrary/manuals/dlm/dlm--pubs.asp>).

“Unique item identifier (UII)” means a set of data elements permanently marked on an item that is globally unique and unambiguous and never changes, in order to provide traceability of the item throughout its total life cycle. The term includes a concatenated UII or a DoD recognized unique identification equivalent.

“Unit acquisition cost” has the meaning given in FAR clause 52.245-1.

(b) Reporting Government-furnished property to the IUID Registry. Except as provided in paragraph (c) of this clause, the Contractor shall report, in accordance with paragraph (f), Government-furnished property to the IUID Registry as follows:--

(1) Up to and including December 31, 2013, report serially managed Government-furnished property with a unit-acquisition cost of \$5,000 or greater.

(2) Beginning January 1, 2014, report—

- (i) All serially managed Government-furnished property, regardless of unit-acquisition cost; and
- (ii) Contractor receipt of non-serially managed items. Unless tracked as an individual item, the Contractor shall report non-serially managed items to the Registry in the same unit of packaging, e.g., original manufacturer's package, box, or container, as it was received.

(c) Exceptions. Paragraph (b) of this clause does not apply to—

- (1) Contractor-acquired property;
- (2) Property under any statutory leasing authority;
- (3) Property to which the Government has acquired a lien or title solely because of partial, advance, progress, or performance-based payments;
- (4) Intellectual property or software;
- (5) Real property; or
- (6) Property released for work in process.

(d) Data for reporting to the IUID Registry. To permit reporting of Government-furnished property to the IUID Registry, the Contractor's property management system shall enable the following data elements in addition to those required by paragraph (f)(1)(iii)(A)(1) through (3), (5), (7), (8), and (10) of the Government Property clause of this contract (FAR 52.245-1):

(1) Received/Sent (shipped) date.

(2) Status code.

(3) Accountable Government contract number.

(4) Commercial and Government Entity (CAGE) code on the accountable Government contract.

(5) Mark record.

(i) Bagged or tagged code (for items too small to individually tag or mark).

(ii) Contents (the type of information recorded on the item, e.g., item internal control number).

(iii) Effective date (date the mark is applied).

(iv) Added or removed code/flag.

(v) Marker code (designates which code is used in the marker identifier, e.g., D=CAGE, UN=DUNS, LD=DODAAC).

(vi) Marker identifier, e.g., Contractor's CAGE code or DUNS number.

(vii) Medium code; how the data is recorded, e.g., barcode, contact memory button.

(viii) Value, e.g., actual text or data string that is recorded in its human-readable form.

(ix) Set (used to group marks when multiple sets exist).

(6) Appropriate supply condition code, required only for reporting of reparable, per Appendix 2 of DoD 4000.25-2-M, Military Standard Transaction Reporting and Accounting Procedures manual (<http://www2.dla.mil/j-6/dlms/eLibrary/manuals/dlm/dlm--pubs.asp>).

(e) When Government-furnished property is in the possession of subcontractors, Contractors shall ensure that reporting is accomplished using the data elements required in paragraph (d) of this clause.

(f) Procedures for reporting of Government-furnished property. Except as provided in paragraph (c) of this clause, the Contractor shall establish and report to the IUID Registry the information required by FAR clause 52.245-1, paragraphs (e) and (f)(1)(iii), in accordance with the data submission procedures at http://www.acq.osd.mil/dpap/pdi/uid/data_submission_information.html.

(g) Procedures for updating the IUID Registry.

(1) Except as provided in paragraph (g)(2), the Contractor shall update the IUID Registry at <https://iuid.logisticsinformationservice.dla.mil/> for changes in status, mark, custody, condition code (for reparable only), or disposition of items that are—

- (i) Received by the Contractor;
 - (ii) Delivered or shipped from the Contractor's plant, under Government instructions, except when shipment is to a subcontractor or other location of the Contractor;
 - (iii) Consumed or expended, reasonably and properly, or otherwise accounted for, in the performance of the contract as determined by the Government property administrator, including reasonable inventory adjustments;
 - (iv) Disposed of; or
 - (v) Transferred to a follow-on or other contract.
- (2) The Contractor need not report to the IUID Registry those transactions reported or to be reported to the following DCMA etools:
- (i) Plant Clearance Automated Reutilization and Screening System (PCARSS); or
 - (ii) Lost, Theft, Damaged or Destroyed (LTDD) system.
- (3) The contractor shall update the IUID Registry as transactions occur or as otherwise stated in the Contractor's property management procedure.

(End of clause)

252.245-7004 REPORTING, REUTILIZATION, AND DISPOSAL (MAR 2015)

(a) Definitions. As used in this clause--

(1) Demilitarization means the act of eliminating the functional capabilities and inherent military design features from DoD personal property. Methods and degree range from removal and destruction of critical features to total destruction by cutting, tearing, crushing, mangling, shredding, melting, burning, etc.

(2) Export-controlled items means items subject to the Export Administration Regulations (EAR) (15 CFR parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120-130). The term includes--

(i) Defense items, defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, etc.; and

(ii) Items, defined in the EAR as ``commodities," ``software," and ``technology," terms that are also defined in the EAR, 15 CFR 772.1.

(3) Ineligible transferees means individuals, entities, or countries--

(i) Excluded from Federal programs by the General Services Administration as identified in the System for Award Management Exclusions located at <https://www.acquisition.gov>;

(ii) Delinquent on obligations to the U.S. Government under surplus sales contracts;

(iii) Designated by the Department of Defense as ineligible, debarred, or suspended from defense contracts; or

(iv) Subject to denial, debarment, or other sanctions under export control laws and related laws and regulations, and orders

administered by the Department of State, the Department of Commerce, the Department of Homeland Security, or the Department of the Treasury.

(4) Scrap means property that has no value except for its basic material content. For purposes of demilitarization, scrap is defined as recyclable waste and discarded materials derived from items that have been rendered useless beyond repair, rehabilitation, or restoration such that the item's original identity, utility, form, fit, and function have been destroyed. Items can be classified as scrap if processed by cutting, tearing, crushing, mangling, shredding, or melting. Intact or recognizable components and parts are not "scrap."

(5) Serviceable or usable property means property with potential for reutilization or sale "as is" or with minor repairs or alterations.

(b) Inventory disposal schedules. Unless disposition instructions are otherwise included in this contract, the Contractor shall complete SF 1428, Inventory Schedule B, within the Plant Clearance Automated Reutilization Screening System (PCARSS). Information on PCARSS can be obtained from the plant clearance officer and at <http://www.dcmamilitary.com/ITCSO/CBT/PCARSS/index.cfm>.

(1) The SF 1428 shall contain the following:

(i) If known, the applicable Federal Supply Code (FSC) for all items, except items in scrap condition.

(ii) If known, the manufacturer name for all aircraft components under Federal Supply Group (FSG) 16 or 17 and FSCs 2620, 2810, 2915, 2925, 2935, 2945, 2995, 4920, 5821, 5826, 5841, 6340, and 6615.

(iii) The manufacturer name, make, model number, model year, and serial number for all aircraft under FSCs 1510 and 1520.

(iv) Appropriate Federal Condition Codes. See Appendix 2 of DLM 4000.25-2, Military Standard Transaction Reporting and Accounting Procedures (MILSTRAP) manual, edition in effect as of the date of this contract. Information on Federal Condition Codes can be obtained at http://www2.dla.mil/j-6/dlmsso/elibrary/manuals/dlm/dlm_pubs.asp#.

(2) If the schedules are acceptable, the plant clearance officer shall complete and send the Contractor a DD Form 1637, Notice of Acceptance of Inventory.

(c) Proceeds from sales of surplus property. Unless otherwise provided in the contract, the proceeds of any sale, purchase, or retention shall be--

(1) Forwarded to the Contracting Officer;

(2) Credited to the Government as part of the settlement agreement;

(3) Credited to the price or cost of the contract; or

(4) Applied as otherwise directed by the Contracting Officer.

(d) Demilitarization, mutilation, and destruction. If demilitarization, mutilation, or destruction of contractor inventory is required, the Contractor shall demilitarize, mutilate, or destroy contractor inventory, in accordance with the terms and conditions of the contract and consistent with Defense Demilitarization Manual, DoDM 4160.28-M, edition in effect as of the date of this contract. The plant clearance officer may authorize the purchaser to demilitarize, mutilate, or destroy as a condition of sale provided the property is not inherently dangerous to public health and safety.

(e) Classified Contractor inventory. The Contractor shall dispose of classified contractor inventory in accordance with applicable security guides and regulations or as directed by the Contracting Officer.

(f) Inherently dangerous Contractor inventory. Contractor inventory dangerous to public health or safety shall not be disposed of unless rendered innocuous or until adequate safeguards are provided.

(g) Contractor inventory located in foreign countries. Consistent with contract terms and conditions, property disposition shall be in accordance with foreign and U.S. laws and regulations, including laws and regulations involving export controls, host nation requirements, Final Governing Standards, and Government-to-Government agreements. The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.

(h) Disposal of scrap.

(1) Contractor with scrap procedures.

(i) The Contractor shall include within its property management procedure, a process for the accountability and management of Government-owned scrap. The process shall, at a minimum, provide for the effective and efficient disposition of scrap, including sales to scrap dealers, so as to minimize costs, maximize sales proceeds, and, contain the necessary internal controls for mitigating the improper release of non-scrap property.

(ii) The Contractor may commingle Government and contractor-owned scrap and provide routine disposal of scrap, with plant clearance officer concurrence, when determined to be effective and efficient.

(2) Scrap warranty. The plant clearance officer may require the Contractor to secure from scrap buyers a DD Form 1639, Scrap Warranty.

(i) Sale of surplus Contractor inventory.

(1) The Contractor shall conduct sales of contractor inventory (both useable property and scrap) in accordance with the requirements of this contract and plant clearance officer direction.

(2) Any sales contracts or other documents transferring title shall include the following statement:

“The Purchaser certifies that the property covered by this contract will be used in (name of country). In the event of resale or export by the Purchaser of any of the property, the Purchaser agrees to obtain the appropriate U.S. and foreign export or re-export license approval.”

(j) Restrictions on purchase or retention of Contractor inventory. (1) The Contractor may not knowingly sell the inventory to any person or that person's agent, employee, or household member if that person--

(i) Is a civilian employee of the DoD or the U.S. Coast Guard;

(ii) Is a member of the armed forces of the United States, including the U.S. Coast Guard; or

(iii) Has any functional or supervisory responsibilities for or within the DoD's property disposal/disposition or plant clearance programs or for the disposal of contractor inventory.

(2) The Contractor may conduct Internet-based sales, to include use of a third party.

(3) If the Contractor wishes to bid on the sale, the Contractor or its employees shall submit bids to the plant clearance officer prior to soliciting bids from other prospective bidders.

(4) The Contractor shall solicit a sufficient number of bidders to obtain adequate competition. Informal bid procedures shall be used, unless the plant clearance officer directs otherwise. The Contractor shall include in its invitation for bids, the sales terms and conditions provided by the plant clearance officer.

(5) The Contractor shall solicit bids at least 15 calendar days before bid opening to allow adequate opportunity to inspect the property and prepare bids.

(6) For large sales, the Contractor may use summary lists of items offered as bid sheets with detailed descriptions attached.

(7) In addition to mailing or delivering notice of the proposed sale to prospective bidders, the Contractor may (when the results are expected to justify the additional expense) display a notice of the proposed sale in appropriate public places, e.g., publish a sales notice on the Internet in appropriate trade journals or magazines and local newspapers.

(8) The plant clearance officer or representative will witness the bid opening. The Contractor shall submit, either electronically or manually, two copies of the bid abstract.

(9) The following terms and conditions shall be included in sales contracts involving the demilitarization, mutilation, or destruction of property:

(i) Demilitarization, mutilation, or destruction on Contractor or subcontractor premises. Item(s) ---- require demilitarization, mutilation, or destruction by the Purchaser. Insert item number(s) and specific demilitarization, mutilation, or destruction requirements for item(s) shown in Defense Demilitarization Manual, DoDM 4160.28-M, edition in effect as of the date of this contract. Demilitarization shall be witnessed and verified by a Government representative using DRMS Form 145 or equivalent.

(ii) Demilitarization, mutilation, or destruction off Contractor or subcontractor premises.

(A) Item(s) ---- require demilitarization, mutilation, or destruction by the Purchaser. Insert item number(s) and specific demilitarization, mutilation, or destruction requirements for item(s) shown in Defense Demilitarization Manual, DoDM 4160.28-M, edition in effect as of the date of this contract. Demilitarization shall be witnessed and verified by a Government representative using DRMS Form 145 or equivalent.

(B) Property requiring demilitarization shall not be removed, and title shall not pass to the Purchaser, until demilitarization has been accomplished and verified by a Government representative. Demilitarization will be accomplished as specified in the sales contract. Demilitarization shall be witnessed and verified by a Government representative using DRMS Form 145 or equivalent.

(C) The Purchaser agrees to assume all costs incident to the demilitarization and to restore the working area to its present condition after removing the demilitarized property.

(iii) Failure to demilitarize. If the Purchaser fails to demilitarize, mutilate, or destroy the property as specified in the contract, the Contractor may, upon giving 10 days written notice from date of mailing to the Purchaser--

(A) Repossess, demilitarize, and return the property to the Purchaser, in which case the Purchaser hereby agrees to pay to the Contractor, prior to the return of the property, all costs incurred by the Contractor in repossessing, demilitarizing, and returning the property;

(B) Repossess, demilitarize, and resell the property, and charge the defaulting Purchaser with all costs incurred by the Contractor. The Contractor shall deduct these costs from the purchase price and refund the balance of the purchase price, if any, to the Purchaser. In the event the costs exceed the purchase price, the defaulting Purchaser hereby agrees to pay these costs to the Contractor; or

(C) Repossess and resell the property under similar terms and conditions. In the event this option is exercised, the Contractor shall charge the defaulting Purchaser with all costs incurred by the Contractor. The Contractor shall

deduct these costs from the original purchase price and refund the balance of the purchase price, if any, to the defaulting Purchaser. Should the excess costs to the Contractor exceed the purchase price, the defaulting Purchaser hereby agrees to pay these costs to the Contractor.

(End of clause)

252.246-7007 CONTRACTOR COUNTERFEIT ELECTRONIC PART DETECTION AND AVOIDANCE SYSTEM
(MAY 2014)

The following paragraphs (a) through (e) of this clause do not apply unless the Contractor is subject to the Cost Accounting Standards under 41 U.S.C. chapter 15, as implemented in regulations found at 48 CFR 9903.201-1.

(a) Definitions. As used in this clause--

Counterfeit electronic part means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

Electronic part means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81). The term "electronic part" includes any embedded software or firmware.

Obsolete electronic part means an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer. Suspect counterfeit electronic part means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.

(b) Acceptable counterfeit electronic part detection and avoidance system. The Contractor shall establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to maintain an acceptable counterfeit electronic part detection and avoidance system, as defined in this clause, may result in disapproval of the purchasing system by the Contracting Officer and/or withholding of payments.

(c) System criteria. A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas:

(1) The training of personnel.

(2) The inspection and testing of electronic parts, including criteria for acceptance and rejection. Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the Government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.

(3) Processes to abolish counterfeit parts proliferation.

(4) Processes for maintaining electronic part traceability (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies. This traceability process shall include certification and traceability documentation developed by manufacturers in accordance with Government and industry standards; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller; and where available, the manufacturer's batch identification for the electronic part(s), such as date codes, lot codes, or serial numbers. If IUID marking is selected as a traceability mechanism, its usage shall comply with the item marking requirements of 252.211-7003, Item Unique Identification and Valuation.

(5) Use of suppliers that are the original manufacturer, or sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria.

(6) Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP) when the Contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DoD, or purchased by a Contractor for delivery to, or on behalf of, the DoD, contains counterfeit electronic parts or suspect counterfeit electronic parts. Counterfeit electronic parts and suspect counterfeit electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic.

(7) Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.

(8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.

(9) Flowdown of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.

(10) Process for keeping continually informed of current counterfeiting information and trends, including detection and avoidance techniques contained in appropriate industry standards, and using such information and techniques for continuously upgrading internal processes.

(11) Process for screening GIDEP reports and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.

(12) Control of obsolete electronic parts in order to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle.

(d) Government review and evaluation of the Contractor's policies and procedures will be accomplished as part of the evaluation of the Contractor's purchasing system in accordance with 252.244-7001, Contractor Purchasing System Administration--Basic, or Contractor Purchasing System Administration--Alternate I.

(e) The Contractor shall include the substance of this clause, including paragraphs (a) through (e), in subcontracts, including subcontracts for commercial items, for electronic parts or assemblies containing electronic parts.

(End of clause)

252.247-7023 TRANSPORTATION OF SUPPLIES BY SEA (APR 2014)

(a) Definitions. As used in this clause --

"Components" means articles, materials, and supplies incorporated directly into end products at any level of manufacture, fabrication, or assembly by the Contractor or any subcontractor.

"Department of Defense" (DoD) means the Army, Navy, Air Force, Marine Corps, and defense agencies.

"Foreign-flag vessel" means any vessel that is not a U.S.-flag vessel.

"Ocean transportation" means any transportation aboard a ship, vessel, boat, barge, or ferry through international waters.

"Subcontractor" means a supplier, materialman, distributor, or vendor at any level below the prime contractor whose contractual obligation to perform results from, or is conditioned upon, award of the prime contract and who is performing any part of the work or other requirement of the prime contract.

"Supplies" means all property, except land and interests in land, that is clearly identifiable for eventual use by or owned by the DoD at the time of transportation by sea.

(i) An item is clearly identifiable for eventual use by the DoD if, for example, the contract documentation contains a reference to a DoD contract number or a military destination.

(ii) "Supplies" includes (but is not limited to) public works; buildings and facilities; ships; floating equipment and vessels of every character, type, and description, with parts, subassemblies, accessories, and equipment; machine tools; material; equipment; stores of all kinds; end items; construction materials; and components of the foregoing.

"U.S.-flag vessel" means a vessel of the United States or belonging to the United States, including any vessel registered or having national status under the laws of the United States.

(b)(1) The Contractor shall use U.S.-flag vessels when transporting any supplies by sea under this contract.

(2) A subcontractor transporting supplies by sea under this contract shall use U.S.-flag vessels if--

(i) This contract is a construction contract; or

(ii) The supplies being transported are--

(A) Noncommercial items; or

(B) Commercial items that--

(1) The Contractor is reselling or distributing to the Government without adding value (generally, the Contractor does not add value to items that it contracts for f.o.b. destination shipment);

(2) Are shipped in direct support of U.S. military contingency operations, exercises, or forces deployed in humanitarian or peacekeeping operations; or

(3) Are commissary or exchange cargoes transported outside of the Defense Transportation System in accordance with 10 U.S.C. 2643.

(c) The Contractor and its subcontractors may request that the Contracting Officer authorize shipment in foreign-flag vessels, or designate available U.S.-flag vessels, if the Contractor or a subcontractor believes that --

- (1) U.S.-flag vessels are not available for timely shipment;
- (2) The freight charges are inordinately excessive or unreasonable; or
- (3) Freight charges are higher than charges to private persons for transportation of like goods.
- (d) The Contractor must submit any request for use of foreign-flag vessels in writing to the Contracting Officer at least 45 days prior to the sailing date necessary to meet its delivery schedules. The Contracting Officer will process requests submitted after such date(s) as expeditiously as possible, but the Contracting Officer's failure to grant approvals to meet the shipper's sailing date will not of itself constitute a compensable delay under this or any other clause of this contract. Requests shall contain at a minimum --

- (1) Type, weight, and cube of cargo;
- (2) Required shipping date;
- (3) Special handling and discharge requirements;
- (4) Loading and discharge points;
- (5) Name of shipper and consignee;
- (6) Prime contract number; and
- (7) A documented description of efforts made to secure U.S.-flag vessels, including points of contact (with names and telephone numbers) with at least two U.S.-flag carriers contacted. Copies of telephone notes, telegraphic and facsimile message or letters will be sufficient for this purpose.
- (e) The Contractor shall, within 30 days after each shipment covered by this clause, provide the Contracting Officer and the Maritime Administration, Office of Cargo Preference, U.S. Department of Transportation, 400 Seventh Street SW., Washington, DC 20590, one copy of the rated on board vessel operating carrier's ocean bill of lading, which shall contain the following information:

- (1) Prime contract number;
- (2) Name of vessel;
- (3) Vessel flag of registry;
- (4) Date of loading;
- (5) Port of loading;
- (6) Port of final discharge;
- (7) Description of commodity;
- (8) Gross weight in pounds and cubic feet if available;
- (9) Total ocean freight in U.S. dollars; and
- (10) Name of the steamship company.

- (f) If this contract exceeds the simplified acquisition threshold, the Contractor shall provide with its final invoice under this contract a representation that to the best of its knowledge and belief--

- (1) No ocean transportation was used in the performance of this contract;
- (2) Ocean transportation was used and only U.S.-flag vessels were used for all ocean shipments under the contract;
- (3) Ocean transportation was used, and the Contractor had the written consent of the Contracting Officer for all foreign-flag ocean transportation; or
- (4) Ocean transportation was used and some or all of the shipments were made on foreign-flag vessels without the written consent of the Contracting Officer. The Contractor shall describe these shipments in the following format:

ITEM DESCRIPTION	CONTRACT LINE ITEMS	QUANTITY
TOTAL _____		

(g) If this contract exceeds the simplified acquisition threshold and the final invoice does not include the required representation, the Government will reject and return it to the Contractor as an improper invoice for the purposes of the Prompt Payment clause of this contract. In the event there has been unauthorized use of foreign-flag vessels in the performance of this contract, the Contracting Officer is entitled to equitably adjust the contract, based on the unauthorized use.

(h) In the award of subcontracts for the types of supplies described in paragraph (b)(2) of this clause, including subcontracts for commercial items, the Contractor shall flow down the requirements of this clause as follows:

- (1) The Contractor shall insert the substance of this clause, including this paragraph (h), in subcontracts that exceed the simplified acquisition threshold in part 2 of the Federal Acquisition Regulation.
- (2) The Contractor shall insert the substance of paragraphs (a) through (e) of this clause, and this paragraph (h), in subcontracts that are at or below the simplified acquisition threshold in part 2 of the Federal Acquisition Regulation.

(End of clause)

252.247-7024 Notification of Transportation of Supplies by Sea (MAR 2000)

(a) The Contractor has indicated by the response to the solicitation provision, Representation of Extent of Transportation by Sea, that it did not anticipate transporting by sea any supplies. If, however, after the award of this contract, the Contractor learns that supplies, as defined in the Transportation of Supplies by Sea clause of this contract, will be transported by sea, the Contractor --

- (1) Shall notify the Contracting Officer of that fact; and
- (2) Hereby agrees to comply with all the terms and conditions of the Transportation of Supplies by Sea clause of this contract.
- (b) The Contractor shall include this clause; including this paragraph (b), revised as necessary to reflect the relationship of the contracting parties--
- (1) In all subcontracts under this contract, if this contract is a construction contract; or

(2) If this contract is not a construction contract, in all subcontracts under this contract that are for--

(i) Noncommercial items; or

(ii) Commercial items that--

(A) The Contractor is reselling or distributing to the Government without adding value (generally, the Contractor does not add value to items that it subcontracts for f.o.b. destination shipment);

(B) Are shipped in direct support of U.S. military contingency operations, exercises, or forces deployed in humanitarian or peacekeeping operations; or

(C) Are commissary or exchange cargoes transported outside of the Defense Transportation System in accordance with 10 U.S.C. 2643.

(End of clause)

252.204-7012

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (SEP 2015)

(a) *Definitions.* As used in this clause—

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Contractor attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Contractor information system” means an information system belonging to, or operated by or for, the Contractor.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified information that—

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) *Controlled technical information.*

(B) *Critical information (operations security)*. Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) *Export control*. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

“Cyber incident” means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

“Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapid(ly) report(ing)” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS [252.227-7013](#), Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

(A) Cloud computing services shall be subject to the security requirements specified in the clause [252.239-7010](#), Cloud Computing Services, of this contract; and

(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract; or

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” <http://dx.doi.org/10.6028/NIST.SP.800-171> that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the DoD CIO prior to contract award; and

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor’s network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor’s ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <http://dibnet.dod.mil>.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <http://dibnet.dod.mil>.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <http://iase.disa.mil/pki/eca/Pages/index.aspx>.

(d) *Malicious software.* The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

- (1) To entities with missions that may be affected by such information;
- (2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- (3) To Government entities that conduct counterintelligence or law enforcement investigations;
- (4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
- (5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at [252.204-7009](#), Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government’s use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor’s responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts.* The Contractor shall—

- (1) Include the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items; and

(2) Require subcontractors to rapidly report cyber incidents directly to DoD at <http://dibnet.dod.mil> and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

Section J - List of Documents, Exhibits and Other Attachments

Exhibit/Attachment Table of Contents

DOCUMENT TYPE	DESCRIPTION	PAGES	DATE
Attachment 1	DD Form 254	20	13-JUN-2016
Attachment 2	Small Business Subcontracting Plan	5	26-MAY-2016

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION (The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)				1. CLEARANCE AND SAFEGUARDING	
				a. FACILITY CLEARANCE REQUIRED TOP SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED SECRET	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)	
X a. PRIME CONTRACT NUMBER N66001-16-D-0205; BCD: 20210629		X a. ORIGINAL (Complete date in all cases)		DATE (YYYYMMDD) 20160613	
b. SUBCONTRACT NUMBER		b. REVISED (Supersedes all previous specs)		REVISION NO. DATE (YYYYMMDD)	
c. SOLICITATION OR OTHER NUMBER N66001-15-R-0037		DUE DATE (YYYYMMDD)		c. FINAL (Complete item 6 in all cases) DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under (Preceding Contract Number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated , retention of the classified material is authorized for the period of					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE SCIENTIFIC RESEARCH CORPORATION 2300 WINDY RIDGE PARKWAY SUITE 400 SOUTH ATLANTA, GA 30339		b. CAGE CODE 0D5A6		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE (DSS) ATLANTA FIELD OFFICE (IOFSA) 1899 POWERS FERRY ROAD STE 330 ATLANTA, GA 30339	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. LOCATION LOCATION PERFORMING WORK, SEE PAGE 3. FOR SCI LOCATIONS / REQUIREMENTS SEE BLOCK 13 PHRASE 10.E(1) ON PAGE 3.		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT SUPPORT OF NETWORKS, COMMUNICATION SYSTEMS, SENSORS, APPLICATIONS AND INFORMATION SYSTEMS THAT ARE CURRENTLY OPERATIONAL, UNDER DEVELOPMENT, REQUIRING UPGRADES OR THEORETICAL.					
10. CONTRACTOR WILL REQUIRE ACCESS TO:					
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
b. RESTRICTED DATA			X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
d. FORMERLY RESTRICTED DATA			X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
e. INTELLIGENCE INFORMATION			X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
(1) Sensitive Compartmented Information (SCI)		X		e. PERFORM SERVICES ONLY	
(2) Non-SCI			X	f. HAVE ACCESS TO ALL CLASSIFIED INFORMATION OUTSIDE THE U.S., EXCEPT FOR U.S. POSSESSIONS AND FIRST CLASSIFIED	
f. SPECIAL ACCESS INFORMATION			X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECURITY DISTRIBUTION CENTER	
g. NATO INFORMATION			X	h. REQUIRE A COMSEC ACCOUNT	
h. FOREIGN GOVERNMENT INFORMATION			X	i. HAVE TEMPORARY REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION			X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
j. FOR OFFICIAL USE ONLY INFORMATION		X		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
k. OTHER (Specify)		X		l. OTHER (Specify)	
NATO BRIEFING FOR SIPRNET/JWICS/NSANET AT GOVERNMENT FACILITY ONLY.				BLOCK 13 FOR ELECTRONIC MEDIA REQUIREMENTS, AT/FP TRAINING, PERFORM NISFOM REQMT. AND UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION REQUIREMENTS.	

013-15 Prime N6600-16-D-0205 SRC 6-29-21

BEVERLY ELLIS
SECURITY SPECIALIST
SPAWARSYSCEN PAC

138

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public release except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☒ Direct ☐ Through (Specify)

COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC (SSC PACIFIC), CODE 85003, 53560
HULL STREET, SAN DIEGO, CA 92152-5001.

RELEASE OF COMSEC AND SCI MATERIAL IS NOT AUTHORIZED.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidelines/references referenced herein. Add additional pages as needed to provide complete guidance.)

PR NO.: SOLICITATION / CONTRACT NUMBER: N66001-15-R-0037 / N66001-16-D-0205

ECD: 20210629

CLASSIFICATION GUIDE: GUIDE TO BE PROVIDED UNDER SEPARATE COVER BY THE COR. OPNAVINST 5513.6, ID # 06-21.1, UHF SATELLITE COMMUNICATIONS (SATCOM); OPNAVINST 5513.8, ID# 08-003.1, ECM/ECCM, GENERAL

ACCESS REQUIREMENTS: (CONTINUED ON PAGES 3 THROUGH 5)

DIRECT SCI QUESTIONS TO THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) IS (b)(6)
CODE 55110, (619) 553-9553, EMAIL: (b)(6) THE CONTRACTING SPECIALIST (CS) IS
MATTHEW SCHUPBACH, CODE 22550, (619) 553-1481, EMAIL: MATTHEW.SCHUPBACH@NAVY.MIL.

PRIME CONTRACTOR'S ARE REQUIRED TO SEND COPIES OF ALL SUBCONTRACT DD FORM 254S TO THE DISTRIBUTION LISTED IN BLOCK 17: SSC PACIFIC CODES 55110 (COR), 22550 (CS), (SEE ABOVE), 83310 SECURITY - (W_SPSC_SSC_PAC_SECURITYCOR_US@NAVY.MIL EXTERNAL ADDRESS).

ALL CLASSIFIED MATERIAL MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER 13526 DTD 5 JANUARY 2010 AND CNO LTR N09N2/8U223000 DTD 7 JAN 08. NOTE: EXEMPTION CATEGORIES X1 THROUGH X8 DECLASSIFICATION MARKINGS ARE NO LONGER USED. YOUR DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY REPRESENTATIVE (IS REP) SHOULD BE CONTACTED FOR ASSISTANCE.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contract clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS ARE ATTACHED AND MUST BE PASSED TO SUBCONTRACTORS.
(CONTINUED ON PAGE 5)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

CSO AND INSPECTION AUTHORITY FOR SCI IS SSO NAVY.

(b)(6)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL (b)(6)	b. TITLE SECURITY'S COR	c. TELEPHONE (Include Area Code) (619) 553-3005
--	----------------------------	--

d. ADDRESS (Include Zip Code)
COMMANDING OFFICER
SSC PACIFIC, CODE 83310
53560 HULL STREET, SAN DIEGO, CA 92152-5001

17. REQUIRED DISTRIBUTION

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR |
| <input checked="" type="checkbox"/> | b. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY SEE BLOCK 13 ABOVE |

(b)(6)

20160613

SCIENTIFIC RESEARCH CORPORATION
SOLICITATION / CONTRACT NUMBERS: N66001-15-R-0037 / N66001-16-D-0205

BLOCK 8A CONTINUATION

PAGE 3 OF 5

SCIENTIFIC RESEARCH CORPORATION
AKA SRC
1101 REMOUNT ROAD
SUITE 500
NORTH CHARLESTON, SC 29406
FCL: TOP SECRET
SAFEGUARDING: SECRET

0Y6T9 DEFENSE SECURITY SERVICE (DSS)
VIRGINIA BEACH FIELD OFFICE (IOFSV)
277 BENDIX ROAD
STE. 200
VIRGINIA BEACH, VA 23452

BLOCK 13 CONTINUATION

ACCESS REQUIREMENTS CONTINUATION:

10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF THE SSC PACIFIC TECHNICAL CODE. ACCESS TO ANY COMSEC INFORMATION REQUIRES SPECIAL BRIEFINGS AT THE CONTRACTOR FACILITY. ACCESS TO CLASSIFIED COMSEC INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL. USE OF COMSEC INFORMATION IS GOVERNED BY THE NSA INDUSTRIAL COMSEC MANUAL, NSA/CSS POLICY MANUAL 3-16. CONTRACTORS THAT WILL BE DESIGNATED CMS USERS MUST ATTEND AN INITIAL CMS USER TRAINING CLASS THAT IS GIVEN BY THE SSC PACIFIC CMS OFFICE. IF YOU HAVE QUESTIONS CALL (819) 553-5065. (ACCESS IS FOR COMSEC EQUIPMENT/MATERIAL.)

10.E(1) THE SSO NAVY HAS EXCLUSIVE SECURITY RESPONSIBILITY FOR ALL SCI CLASSIFIED MATERIAL RELEASED OR DEVELOPED UNDER THIS CONTRACT. DSS IS RELIEVED OF SECURITY INSPECTION RESPONSIBILITY FOR ALL SUCH MATERIAL BUT RETAINS RESPONSIBILITY FOR ALL NON-SCI CLASSIFIED MATERIAL RELEASED TO OR DEVELOPED UNDER THIS CONTRACT. FURTHER DISCLOSURE TO INCLUDE SUBCONTRACTING OF SCI IS PROHIBITED WITHOUT PRIOR APPROVAL FROM THE SSC PACIFIC, TECHNICAL COR-CODE, SSC PACIFIC CODE 874 AND SSO NAVY. SPECIAL BRIEFINGS AND PROCEDURES ARE ALL REQUIRED AT THE CONTRACTOR'S FACILITY. ACCESS TO SCI INFORMATION REQUIRES A FINAL US GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL AND WILL BE PERFORMED WITHIN U.S. GOVERNMENT FACILITIES ONLY. INCIDENTAL SCI VALIDATION ACCESS RECEIVED FROM SSO NAVY/JRCCO TO PROCESS THIS SOLICITATION. PACKAGE SUBMITTED FOR INCIDENTAL SCI ACCESS FOR PRIME CONTRACTOR.

CONTRACTOR PERSONNEL ASSIGNED TO THIS EFFORT WHO REQUIRE ACCESS TO SCI DATA AND SPACES MUST POSSESS A CURRENT SSBI WITH ICD 704 ELIGIBILITY (WHICH REPLACED DCID 6/4 ELIGIBILITY).

CONTRACT PERFORMANCE FOR INCIDENTAL SCI ACCESS IS RESTRICTED TO: SSC PACIFIC, SAN DIEGO, CA.

10.K CONTRACTOR IS REQUIRED TO BE NATO BRIEFED FOR THE SOLE PURPOSE OF ACCESSING SIPRNET/JWICS/NSANET. THE SPECIAL BRIEFING IS PROVIDED BY THE CONTRACTING COMPANY'S FACILITY SECURITY OFFICER. NOTE: THERE IS NO REQUIREMENT FOR THE CONTRACTOR TO HAVE ACCESS TO NATO MATERIAL ON THIS CONTRACT PER CNO LTR 5510 SER N05N2/11U213075 DTD 9 SEP 11 THIS INFORMATION IS NOT TO BE ENTERED INTO JPAS. THE CONTRACTOR SHALL COMPLETE DERIVATIVE CLASSIFICATION TRAINING PRIOR TO BEING GRANTED ACCESS TO SIPRNET/JWICS/NSANET; TRAINING PROVIDED BY THE FACILITY SECURITY OFFICER.

11.C ALL CLASSIFIED MATERIAL MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER 13526 DTD 5 JANUARY 2010 AND CNO LTR N09N2/BU223000 DTD 7 JAN 08. NOTE: EXEMPTION CATEGORIES X1 THROUGH X8 DECLASSIFICATION MARKINGS ARE NO LONGER USED.

11.D APPROXIMATELY 2 CUFT OF GSA APPROVED STORAGE WILL BE REQUIRED ON THIS CONTRACT.

11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS LOCATIONS: U.K, GERMANY, FRANCE, ITALY, SAHRAIN, JAPAN, CANADA, SOUTH KOREA, AUSTRALIA, MEXICO, PHILIPPINES, SINGAPORE, IRAQ, AFHAGAN, ANTI-TERRORISM/FORCE PROTECTION BRIEFINGS ARE REQUIRED FOR ALL PERSONNEL (MILITARY, DOD CIVILIAN, AND CONTRACTOR) PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL. THE BRIEFING IS AVAILABLE AT [HTTPS://ATLEVEL1.DTIC.MIL/AT/](https://atlevel1.dtic.mil/at/), IF EXPERIENCING PROBLEMS ACCESSING THIS WEBSITE CONTACT SSC_FORTTRAV@NAVY.MIL. NOTE: PER OPNAVINST F3300.53C CONTRACTOR EMPLOYEES MUST RECEIVE THE AT/FP BRIEFING ANNUALLY. SERE 100.1 LEVEL A CODE OF CONDUCT TRAINING IS ALSO REQUIRED PRIOR TO OCONUS TRAVEL FOR ALL PERSONNEL. SERE 100.1 LEVEL A TRAINING CAN BE ACCESSED AT [HTTPS://WWW.NKO.NAVY.MIL](https://www.nko.navy.mil). PERSONNEL UTILIZING THIS SITE MUST HAVE A CAC. A SERE 100.1 LEVEL A TRAINING DISK CAN BE BORROWED AT THE SSC PACIFIC POINT LOMA OFFICE OR OLD TOWN CAMPUS OFFICE. SPECIALIZED TRAINING FOR SPECIFIC LOCATIONS, SUCH AS SOUTHCOM HUMAN RIGHTS, OR U.S. FORCES KOREA ENTRY TRAINING, MAY ALSO BE REQUIRED; SSC PACIFIC

SCIENTIFIC RESEARCH CORPORATION
SOLICITATION / CONTRACT NUMBERS: N66001-15-R-0037 / N66001-16-D-0205

BLOCK 13 CONTINUATION

PAGE 4 OF 5

PHRASE 11.F CONTINUED:

SECURITY PERSONNEL WILL INFORM YOU IF THERE ARE ADDITIONAL TRAINING REQUIREMENTS. NOTE: PER OPNAVINST F3300.53C CONTRACTOR EMPLOYEES MUST RECEIVE THE AT/FP BRIEFING ANNUALLY. FORWARD A COPY OF TRAINING CERTIFICATE TO THE PREVIOUS EMAIL ADDRESS OR FAX TO (619) 553-6863. FINALLY, EUCOM HAS MANDATED THAT ALL PERSONNEL GOING ON OFFICIAL TRAVEL TO THE EUCOM AOR MUST NOW REGISTER WITH THE SMART TRAVELER ENROLLMENT PROGRAM (STEP). WHEN YOU SIGN UP, YOU WILL AUTOMATICALLY RECEIVE THE MOST CURRENT INFORMATION THE STATE DEPARTMENT COMPILES ABOUT YOUR DESTINATION COUNTRY. YOU WILL ALSO RECEIVE UPDATES, INCLUDING TRAVEL WARNINGS AND TRAVEL ALERTS. SIGN UP IS ONE-TIME ONLY, AFTER YOU HAVE ESTABLISHED YOUR STEP ACCOUNT, YOU CAN EASILY ADD OFFICIAL OR PERSONAL TRAVEL TO ANYWHERE IN THE WORLD, NOT JUST EUCOM: [HTTP://TRAVEL.STATE.GOV/CONTENT/PASSPORTS/EN/GO/STEP.HTML](http://TRAVEL.STATE.GOV/CONTENT/PASSPORTS/EN/GO/STEP.HTML)

11.K THE SSC PACIFIC TECHNICAL POC APPROVES AUTHORIZATION FOR CONTRACTOR TO HAVE A DEFENSE COURIER SERVICE (DCS) ACCOUNT WITH PRIOR VALIDATION. THE CONTRACTOR SHALL MAKE ARRANGEMENTS TO USE THE SERVICES OF THE DCS FOR TRANSPORTATION OF QUALIFIED MATERIAL. THE CONTRACTING ACTIVITY WILL REQUEST DCS SERVICES FROM COMMANDER, DCS, ATTN: OPERATIONS DIVISION, FORT GEORGE MEADE, MD 20755-5370. TO OBTAIN DCS GUIDANCE REFER TO THE DOD DIRECTIVE 5200.33, DEFENSE COURIER SERVICE LOCATED AT [HTTP://WWW.DTIC.MIL/WHIS/DIRECTIVES/CORRES/IDF/520033P.PDF](http://WWW.DTIC.MIL/WHIS/DIRECTIVES/CORRES/IDF/520033P.PDF).

11.L(1) THE USE OF PERSONAL ELECTRONIC MEDIA (COMPUTER LAPTOPS, FLASH (THUMB), OR OTHER REMOVABLE DRIVES) IS PROHIBITED IN SSC PACIFIC SPACES. CONTACT THE COMMAND INFORMATION SYSTEM SECURITY MANAGER (SPSC_SSPAC_ISSM@NAVY.MIL) IF YOU HAVE QUESTIONS. ALL REMOVABLE ELECTRONIC MEDIA MUST BE LABELED (UNCLASSIFIED, ETC.) TO THE HIGHEST CLASSIFICATION OF DATA STORED; AND/OR FOR THE CLASSIFICATION OF THE SYSTEM IN WHICH IT IS USED. IF CLASSIFIED, ANY REMOVABLE ELECTRONIC MEDIA MUST BE TRACKED AND STORED APPROPRIATE TO THAT LEVEL OF CLASSIFICATION.

11.L(2) ANTI-TERRORISM/FORCE PROTECTION BRIEFINGS ARE REQUIRED FOR ALL PERSONNEL (MILITARY, DOD CIVILIAN, AND CONTRACTOR) PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL. THE BRIEFING IS AVAILABLE AT [HTTPS://ATLEVEL1.DTIC.MIL/AT/](https://atlevel1.dtic.mil/at/). IF EXPERIENCING PROBLEMS ACCESSING THIS WEBSITE CONTACT SSC_FORTTRAV@NAVY.MIL. NOTE: PER OPNAVINST F3300.53C CONTRACTOR EMPLOYEES MUST RECEIVE THE AT/FP BRIEFING ANNUALLY. FORWARD A COPY OF TRAINING CERTIFICATE TO THE PREVIOUS EMAIL ADDRESS OR FAX TO (619) 553-6863.

11.L(3) AS REQUIRED BY NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM) CHAPTER 1, SECTION 3, CONTRACTORS ARE REQUIRED TO REPORT CERTAIN EVENTS THAT HAVE AN IMPACT ON: 1) THE STATUS OF THE FACILITY CLEARANCE (FCL); 2) THE STATUS OF AN EMPLOYEE'S PERSONNEL CLEARANCE (PCL); 3) THE PROPER SAFEGUARDING OF CLASSIFIED INFORMATION; 4) OR AN INDICATION THAT CLASSIFIED INFORMATION HAS BEEN LOST OR COMPROMISED. CONTRACTORS WORKING UNDER SSC PACIFIC CONTRACTS WILL ENSURE INFORMATION PERTAINING TO ASSIGNED CONTRACTOR PERSONNEL ARE REPORTED TO THE CONTRACTING OFFICER REPRESENTATIVE (COR)/TECHNICAL POINT OF CONTACT (TPOC), THE CONTRACTING SPECIALIST, AND THE SECURITY'S COR IN ADDITION TO NOTIFYING APPROPRIATE AGENCIES SUCH AS COGNIZANT SECURITY AGENCY (CSA), COGNIZANT SECURITY OFFICE (CSO), OR DEPARTMENT OF DEFENSE CENTRAL ADJUDICATION FACILITY (DODCAF) WHEN THAT INFORMATION RELATES TO THE DENIAL, SUSPENSION, OR REVOCATION OF A SECURITY CLEARANCE OF ANY ASSIGNED PERSONNEL; ANY ADVERSE INFORMATION ON AN ASSIGNED EMPLOYEE'S CONTINUED SUITABILITY FOR CONTINUED ACCESS TO CLASSIFIED ACCESS; ANY INSTANCE OF LOSS OR COMPROMISE, OR SUSPECTED LOSS OR COMPROMISE, OF CLASSIFIED INFORMATION; ACTUAL, PROBABLE OR POSSIBLE ESPIONAGE, SABOTAGE, OR SUBVERSIVE INFORMATION; OR ANY OTHER CIRCUMSTANCES OF A SECURITY NATURE THAT WOULD AFFECT THE CONTRACTOR'S OPERATION WHILE WORKING UNDER SSC PACIFIC CONTRACTS.

11.L(4) CONTRACTORS RECEIVING, TRANSMITTING OR ACCESSING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION ON OR THROUGH ITS CONTRACTOR INFORMATION SYSTEM(S) MUST SAFEGUARD THE INFORMATION TO AVOID COMPROMISE, INCLUDING BUT NOT LIMITED TO DISCLOSURE OF INFORMATION TO UNAUTHORIZED PERSONS, UNAUTHORIZED MODIFICATION, DESTRUCTION, OR LOSS OF AN OBJECT, OR THE COPYING OF INFORMATION TO UNAUTHORIZED MEDIA, AS REQUIRED PER DFARS SUBPART 204.73 AND CLAUSES 204.7304 AND 252.204-7012. CONTRACTORS SHALL REPORT TO THE DOD EACH CYBER INCIDENT THAT AFFECTS UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION RESIDENT ON OR TRANSITING CONTRACTOR INFORMATION SYSTEMS IN ACCORDANCE WITH DFARS CLAUSE 204.7304 AND 252.204-7012. DETAILED REPORTING CRITERIA AND REQUIREMENTS ARE SET FORTH IN THE CLAUSE AT 252.204-7012, SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION. REQUIREMENTS FOR SAFEGUARDING UNCLASSIFIED CONTROLLED INFORMATION CAN BE FOUND IN DOD M-5200.01, VOLUME 4.

SCIENTIFIC RESEARCH CORPORATION
SOLICITATION / CONTRACT NUMBERS: N68001-15-R-0037 / N68001-16-D-0205

BLOCK 13 CONTINUATION

PAGE 5 OF 5

11.4(5) USFF FORCE PROTECTION (FP) DIRECTIVE MSG 16-00 DIRECTS ALL PERSONNEL (MILITARY, DOD CIVILIAN, AND CONTRACTOR) WORKING AT MILITARY FACILITIES TO COMPLETE THE TRAINING AND READINESS - THE ACTIVE SHOOTER. THE TRAINING IS AVAILABLE AT [HTTPS://WWW.WANKO.NAVY.MIL/](https://www.wanko.navy.mil/). YOU WILL FIND THE TRAINING UNDER COURSE CATALOG "PREFDC CNIC, NUMBER: CNIC-TRATAS-1.1.", IF EXPERIENCING PROBLEMS ACCESSING THIS WEBSITE CONTACT SSC_FORTTRAV@NAVY.MIL.

CHANGES: DD254 SUBMITTED REQUESTING APPROVAL/VALIDATION FOR PRIME CONTRACTOR NOTED IN BLOCK 8.A ONLY TO HAVE INCIDENTAL SCI ACCESS. SSO NAVY APPROVAL/VALIDATION #013-16 ATTACHED FOR THE SOLICITATION.

BLOCK 14 CONTINUATION:

SPECIFIC ON-SITE SECURITY REQUIREMENTS ARE ATTACHED. FOR AUTHORIZED VISITS TO OTHER U.S. GOVERNMENT ACTIVITIES, THE CONTRACTOR MUST COMPLY WITH ALL ONSITE SECURITY REQUIREMENTS OF THE HOST COMMAND. INTELLIGENCE REQUIREMENTS ARE ATTACHED.

FOR OFFICIAL USE ONLY (FOUO) GUIDANCE ATTACHED.

OPERATIONS SECURITY (OPSEC) REQUIREMENTS ATTACHED AND MUST BE PASSED TO ALL SUBCONTRACTORS.

DODM 5105.21 VOLUMES 1 THROUGH 3, "DEPARTMENT OF DEFENSE SENSITIVE COMPARTMENTED INFORMATION ADMINISTRATIVE SECURITY MANUAL: ADMINISTRATION OF INFORMATION AND INFORMATION SYSTEMS SECURITY", "ADMINISTRATION OF PHYSICAL SECURITY, VISITOR CONTROL, AND TECHNICAL", AND "ADMINISTRATION OF PERSONNEL SECURITY, INDUSTRIAL SECURITY, AND SPECIAL ACTIVITIES", DATED 19 OCTOBER 2012 (THESE PUBLICATIONS MAY BE OBTAINED BY ACCESSING WEBSITE AT [HTTP://WWW.DTIC.MIL/WHs/DIRECTIVES](http://www.dtic.mil/whs/directives)). DISTRIBUTION IS UNLIMITED APPROVED FOR PUBLIC RELEASE.

NO FURTHER ENTRIES ON THIS PAGE.

DEC-09-2014 08:22

P.002

013-15

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION (The requirements of this DoD Industrial Security Manual apply to all security aspects of this effort.)		1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARDING REQUIRED SECRET	
2. THIS SPECIFICATION IS FOR: (Complete as applicable)		2. THIS SPECIFICATION IS: (Complete as applicable)	
a. PRIME CONTRACT NUMBER	<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date to all copies)	DATE (YYYYMMDD) 20141208
b. OLD CONTRACT NUMBER		b. REVISION (Complete date of previous issue)	DATE (YYYYMMDD)
c. SOLICITATION OR OTHER NUMBER	<input checked="" type="checkbox"/>	c. FINAL (Complete date of release)	DATE (YYYYMMDD)
DATE (YYYYMMDD)			
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under: (Provide Contract Number) is transferred to this follow-on contract.			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated: Attention of the classified material be authorized for the period of:			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)			
a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. DOMINANT SECURITY OFFICE (Name, Address, and Zip Code)	
THIS DD 254 IS FOR SOLICITATION PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE PROVIDED UPON CONTRACT AWARD.			
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. DOMINANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE			
a. LOCATION TO BE NOTED UPON CONTRACT AWARD OR ON INDIVIDUAL TASK ORDERS. FOR SCI REQUIREMENTS SEE BLOCK 15 AND PAGE 1.	b. CAGE CODE	c. DOMINANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT SUPPORT OF NETWORKS, COMMUNICATION SYSTEMS, SENSORS, APPLICATIONS AND INFORMATION SYSTEMS THAT ARE CURRENTLY OPERATIONAL, UNDER DEVELOPMENT, REQUIRING UPGRADES OR THEORETICAL.			
10. CONTRACTOR WILL REQUIRE ACCESS TO:			
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	b. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
b. RESTRICTED DATA	<input checked="" type="checkbox"/>	c. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input checked="" type="checkbox"/>	d. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
d. NONRESTRICTED DATA	<input checked="" type="checkbox"/>	e. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION	<input checked="" type="checkbox"/>	f. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
(1) Unrestricted	<input checked="" type="checkbox"/>	g. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
(2) Restricted	<input checked="" type="checkbox"/>	h. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input checked="" type="checkbox"/>	i. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
g. NAVO INFORMATION	<input checked="" type="checkbox"/>	j. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input checked="" type="checkbox"/>	k. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input checked="" type="checkbox"/>	l. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	m. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
k. OTHER (Specify)	<input checked="" type="checkbox"/>	n. RECEIVING AND/OR TRANSMITTING EQUIPMENT	<input checked="" type="checkbox"/>
BLOCK 10, Q IS YES FOR SIF/NETWORKS/NSA/ST AT GOVERNMENT FACILITY.			

DD FORM 254, DEC 1965

PREVIOUS EDITIONS IS OBSOLETE.

Addendum 12

DEC-09-2014 08:22
013-15 Soli N66001-15-R-0037 FY20

P.003

013-15

12. PUBLIC RELEASE. Any information (submitted or transmitted) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release. ☒ Direct ☐ Through (Specify):

COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC (SSC PACIFIC), CODE 83003, 3360 HULL STREET, SAN DIEGO, CA 92152-5801.

RELEASE OF COMSEC AND SCI MATERIAL IS NOT AUTHORIZED.

In the Department for Protection of Information and Security Window, Office of the Assistant Secretary of Defense (Public Affairs) for review. In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other controlling regulation indicates a need for changes in this guidance, the contractor is encouraged to provide recommended changes to the guidance or the classification assigned to any information or material furnished or generated under this contract and to submit any questions for clarification to the official identified below. Pending final decision, the information involved shall be handled and protected as the highest level of classification assigned or recommended. If it is an appropriate for the classified effort, Attach, or forwards under separate correspondence, any documents/policy materials referenced herein. Add additional pages as needed to provide complete guidance.

PR NO.:

SOLICITATION / CONTRACT NUMBER: N66001-15-R-0037

BCD: TO BE PROVIDED UPON CONTRACT AWARD.

CLASSIFICATION GUIDE: GUIDE TO BE PROVIDED UNDER SEPARATE COVER BY THE COR. OPNAVINST 5513.6, ID # 06-21.1, UHF SATELLITE COMMUNICATIONS (SATCOM); OPNAVINST 5513.8, ID# 08-003.2, ECM/ECCM, GENERAL.

ACCESS REQUIREMENTS: (CONTINUED ON PAGE 5)

DIRECT SCI QUESTIONS TO THE CONTRACTING OFFICER'S REPRESENTATIVE (COR)

(b)(6)

CODE #9116, (619) 524-9616, EMAIL:

(b)(6)

THE CONTRACTING SPECIALIST (CS) IS SEAN KEARNS, CODE 22550, (619) 553-1812.

EMAIL: SEANKEARNS@NAVY.MIL.

PRIME CONTRACTORS ARE REQUIRED TO SEND COPIES OF ALL SUBCONTRACT DD FORM 254S TO THE DISTRIBUTION LISTED IN BLOCK 17: SSC PACIFIC CODES 55116 (COR), 22550 (CS), (SEE ABOVE), 83216 (SECURITY - W_SPSC_SSC_PAC_SECURITYCOR_US@NAVY.MIL).

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to those requirements, are specified for this contract. ☒ Yes ☐ No (If Yes, identify the pertinent operational elements, the control element itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognate security office. Use DD FORM 13 if additional space is needed.)

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS ARE ATTACHED AND MUST BE PASSED TO SUBCONTRACTORS. (CONTINUED ON PAGE 4)

15. INSPECTIONS. Elements of this program are outside the inspection responsibility of the cognate security office. ☒ Yes ☐ No (If Yes, explain and identify specific areas or elements covered and the entity responsible for inspection. Use form 13 if additional space is needed.)

CSO AND INSPECTION AUTHORITY FOR SCI IS SSO NAVY.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CONTROLLING OFFICIAL (b)(6)	b. TITLE SECURITY'S COR	c. TELEPHONE (Include Area Code) (619) 553-3005
d. ADDRESS (Include Zip Code) COMMANDING OFFICER, SSC PACIFIC, CODE 83003 3360 HULL STREET, SAN DIEGO, CA 92152-5801		e. SIGNATURE (b)(6) 2014/203
17. REQUIRED DISTRIBUTION		
<input checked="" type="checkbox"/> a. CONTRACTOR		
<input checked="" type="checkbox"/> b. SUBCONTRACTOR		
<input checked="" type="checkbox"/> c. COORDINATE SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR		
<input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR CIPHERS SECURITY ADMINISTRATION		
<input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER		
<input checked="" type="checkbox"/> f. OTHERS AS NECESSARY SEE BLOCK 13 ABOVE		

DD FORM 254 (BACK), DEC 1989

(b)(6)

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS

The U.S. Government conducts trustworthiness investigations of personnel who are assigned to positions that directly or indirectly affect the operation of unclassified IT resources and systems that process Department of Defense (DoD) Information, to include For Official Use Only (FOUO) and other controlled unclassified information.

The United States Office of Personnel Management (OPM), Federal Investigations Processing Center (FIPC) process all requests for U.S. Government trustworthiness investigations. Requirements for these investigations are outlined in paragraph C3.6.15 and Appendix 10 of DoD 5200.2-R, available at <http://www.dtic.mil/whs/directives/corres/dir.html>. Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories listed below. The contractor shall include all of these requirements in any subcontracts involving IT support. (Note: Terminology used in DoD 5200.2-R references "ADP" vice "IT". For purposes of this requirement, the terms ADP and IT are synonymous.)

The Program Manager (PM), Contracting Officer's Representative (COR) or Technical Representative (TR) shall determine if they or the contractor shall assign the IT Position category to contractor personnel and inform the contractor of their determination. If it is decided the contractor shall make the assignment, the PM, COR, or TR must concur with the designation.

DoDD Directive 8500.01E, Subject: Information Assurance (IA), paragraph 4.8 states "Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information" in accordance with DoDM 5200.01 Vol. 1. DoD 5200.2-R and DoDD 5200.2 require all persons assigned to sensitive positions or assigned to sensitive duties be U.S. citizens. All persons assigned to IT-I and IT-II positions, as well as all persons with access to controlled unclassified information (without regard to degree of IT access) or performing other duties that are considered "sensitive" as defined in DoDD 5200.2 and DoD 5200.2-R must be U.S. citizens. Furthermore, access by non-U.S. citizens to unclassified export controlled data will only be granted to persons pursuant to the export control laws of the U.S. The categories of controlled unclassified information are specified in DoDM 5200.01 Vol. 4. These same restrictions apply to "Representatives of a Foreign Interest" as defined by DoD 5220.22-M (National Industrial Security Program Operating Manual, NISPOM). DoD 8570.01-M further stipulates additional training and/or certification that is required by all persons assigned to Information Assurance functions.

Criteria For Designating Positions:

IT-I Position (Privileged)

- Responsibility for the development and administration of Government computer security programs, and including direction and control of risk analysis and/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT-I category to ensure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
- Other positions as designated by Space and Naval Warfare Systems Center Pacific (SSC Pacific) that involve relatively high risk for effecting grave damage or realizing significant personal gain.

Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated every 5 years by using the Electronic Questionnaire for Investigation Processing (eQIP) web based program (SF86 format).

IT-II Position (Limited Privileged)

Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the IT-I category, includes but is not limited to:

- Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
- Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year. Other positions are designated by Space and Naval Warfare Systems Center Pacific (SSC Pacific) that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT-I positions. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check with Local Agency Check and Credit Check (NACLC).

IT-III Position (Non-Privileged)

- All other positions involving Federal IT activities. Incumbent in this position has non-privileged access to one or more DoD information systems, application, or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated National Agency Check with Inquiries (NACI).

Qualified Cleared Personnel Do NOT Require Trustworthiness Investigations:

When background investigations supporting clearance eligibility have been submitted and/or adjudicated to support assignment to sensitive national security positions, a separate investigation to support IT access will normally not be required. A determination that an individual is NOT eligible for assignment to a position of trust will also result in the removal of eligibility for security clearance. Likewise, a determination that an individual is NOT eligible for a security clearance will result in the denial of eligibility for a position of trust.

Procedures for submitting U.S. Government Trustworthiness Investigations:

Only the e-QIP version of SF-85 and SF 86 are acceptable by OPM-FIPC.

The Facility Security Officer (FSO) must verify employee's security clearance eligibility in the Joint Personnel Adjudication System (JPAS) before contacting SSC Pacific Personnel Security Office to initiate request for trustworthiness investigations.

After determining that an individual requires Public Trust Position determination, the FSO will identify the individual to the SSC Pacific Personnel Security Office and the specific IT Level category assigned for requesting the appropriate type of investigation. The FSO will also provide the following information to the SSC Pacific Personnel Security Office to initiate a request thru e-QIP:

Full SSN of the applicant
Full Name
Date of Birth
Place of Birth
Email Address
Phone Number

The Personnel Security Office will send email notification and instruction to the applicant to complete and submit e-QIP *expeditiously*.

The FSO or SSC Pacific Security will take and submit fingerprints using SF-87, FD-258 or electronic submission. The FSO must obtain from SSC Pacific Personnel Security Office the e-QIP Request Number for inclusion in submitting the fingerprints. *For immediate fingerprint result, electronic transmission of fingerprints is encouraged.* Submission of hard copy SF-87 or FD-258 is acceptable until 2013 to:

E-QIP RAPID RESPONSE TEAM
OPM-FIPC
1137 BRANCHTON ROAD
BOYERS, PA 16020

SSC Pacific Personnel Security Office will notify the FSO when the Public Trust investigation request is released to the Parent Agency, the Office of Personnel Management (OPM).

Contractor fitness determinations made by the DoN CAF are maintained in the Joint Personnel Adjudication System (JPAS). Favorable fitness determinations will support public trust positions only and not national security eligibility. If no issues are discovered, according to respective guidelines a "Favorable Determination" will be populated in JPAS and will be reciprocal within DoN. If issues are discovered, the DoN CAF will place a "No Determination Made" in the JPAS and forward the investigation to the submitting office for the commander's final determination."

For Trustworthiness Investigations that have been returned to the SSC Pacific Security Office with a "No Determination Made" decision, your company will be notified in writing. If an individual received a negative trustworthiness determination, they will be immediately removed from their position of trust, the contractor will follow the same employee termination processing above, and they will replace any individual who has received a negative trustworthiness determination.

If you require additional assistance with the submission of Public Trust Investigations, you may send an email to SSC Pacific at W SPSC SSC PAC clearance US@navy.mil.

Visit Authorization Letters (VALs) for Qualified Employees:

Contractors that have been awarded a classified contract must submit visit requests using "only" the Joint Personnel Adjudication System (JPAS). All government activities have been directed to use JPAS when transmitting or receiving VALS. Therefore, contractors who work on classified contracts are required to have established an account through JPAS for their facility. This database contains all U.S. citizens who have received a clearance of Confidential, Secret, and/or Top Secret. The visit request can be submitted for one year. When submitting a visit requests to SSC Pacific, use its Security Management Office (SMO) number (660015). This information is provided in accordance with guidance provided to contractors via the Defense Security Service (DSS) website <https://www.dss.mil/> (DSS guidance dated 24 April 2007, subject: *Procedures Governing the Use of JPAS by Cleared Contractors*).

Employment Terminations:

The contractor shall:

- Immediately notify the COR or TR of the employee's termination.
- Send email to W SPSC SSC PAC clearance US@navy.mil, Code 83310 notifying them of the termination.
- Fax a termination VAL to Code 83320 at (619) 553-8169.
- Return any badge and decal to Commanding Officer, Space and Naval Warfare Systems Center Pacific, Attn: Code 83320, 53580 Hull Street, San Diego, CA 92152-5001.

SPECIFIC ON-SITE SECURITY REQUIREMENTS

I. GENERAL

- a. **Contractor Performance.** In performance of this Contract the following security services and procedures are incorporated as an attachment to the DD 254. The Contractor will conform to the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program, Operating Manual (NISPOM), as revised. The Contractor will follow all export laws and regulations in the performance of this contract. When visiting Space and Naval Warfare Systems Center Pacific (SSC Pacific) at either the Point Loma Campus (PLC) or Old Town Campus (OTC) the Contractor will comply with the security directives used regarding the protection of classified and controlled unclassified information, SECNAV M-5510.36 (series), SECNAV M-5510.30 (series), DOD M-5200.01 Volumes 1 through 4, and SSCPACINST 5720.1A (series). Both of the SECNAV Instructions and Manuals are available online at <http://doni.daps.dla.mil/SECNAV.aspx> and the DOD Instructions can be found at <http://www.dtic.mil/whs/directives/corres/pub1.html>. A copy of SSCPACINST 5720.1A will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the SSC Pacific Security's Contracting Officer's Representative (COR), Code 83310. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location at SSC Pacific, the security provisions of the NISPOM will be followed within this cleared facility.
- b. **Security Supervision.** SSC Pacific will exercise security supervision over all contractors visiting SSC Pacific and will provide security support to the Contractor as noted below. The Contractor will identify, in writing to Security's COR, an on-site Point of Contact to interface with Security's COR.

II. HANDLING CLASSIFIED MATERIAL OR INFORMATION.

- a. **Control and Safeguarding.** Contractor personnel located at SSC Pacific are responsible for the control and safeguarding of all classified material in their possession. All contractor personnel will be briefed by their FSO on their individual responsibilities to safeguard classified material. In addition, all contractor personnel are invited to attend SSC Pacific conducted Security Briefings, available at this time by appointment only. In the event of possible or actual loss or compromise of classified material, the on-site Contractor will immediately report the incident to SSC Pacific Code 83310, (619) 553-3005, as well as the Contractor's FSO. A security specialist, Code 83310 representative will investigate the circumstances, determine culpability where possible, and report results of the inquiry to the FSO and the Cognizant Field Office of the DSS. On-site contractor personnel will promptly correct any deficient security conditions identified by a SSC Pacific Security representative.
- b. **Storage.**
 1. Classified material may be stored in containers authorized by SSC Pacific PLC Physical Security Group, Code 83320 for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board SSC Pacific PLC with Code 83320's written permission. Areas located within cleared contractor facilities on board SSC Pacific will be approved by DSS.
 2. The use of Open Storage areas must be pre-approved in writing by Code 83320 for the open storage, or processing, of classified material prior to use of that area for open storage. Specific supplemental security controls for open storage areas, when required, will be provided by SSC Pacific, Code 83320.
- c. **Transmission of Classified Material.**
 1. All classified material transmitted by mail for use by long term visitors will be addressed as follows:
 - (a) TOP SECRET, Non-Sensitive Compartmented Information (SCI) material using the Defense Courier Service: SPAWARSYSCEN-PACIFIC; 271582-SN00, SPAWARSYSCEN PACIFIC.
 - (b) CONFIDENTIAL and SECRET material transmitted by FedEx will be addressed to COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC, ATTN RECEIVING OFFICER CODE 43150, 4297 PACIFIC HIGHWAY, SAN DIEGO, CA 92110.
 - (c) CONFIDENTIAL and SECRET material transmitted by USPS Registered and Express mail will be

addressed to COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC, 53560 HULL STREET, SAN DIEGO CA 92152-5001. The inner envelope will be addressed to the attention of the Contracting Officer's Representative (COR) or applicable Technical Representative (TR) for this contract, to include their code number.

2. All SECRET material hand carried to SSC Pacific by contractor personnel must be delivered to the Classified Material Control Center (CMCC), Code 83430, Building 58, Room 102, for processing.
 3. All CONFIDENTIAL material hand carried to SSC Pacific by contractor personnel must be delivered to the Mail Distribution Center, Code 83430, for processing. This applies for either the QTC or PLC sites.
 4. All SSC Pacific classified material transmitted by contractor personnel from the SSC Pacific will be sent via SSC Pacific COR or TR for this contract.
 5. The sole exception to the above is items categorized as a Data Deliverable. All contract Data Deliverables will be addressed to COMMANDING OFFICER, ATTN DOCUMENT CONTROL CODE 83430, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC, 53560 HULL STREET, SAN DIEGO, CA 92152-5001.
- III. INFORMATION SYSTEMS (IS) Security: Contractors using ISs, networks, or computer resources to process classified, sensitive unclassified and/or unclassified information will comply with the provisions of SECNAVINST 5239.3 (series) and local policies and procedures. Contractor personnel must ensure that systems they use at SSC Pacific have been granted a formal letter of approval to operate by contacting their Information System Security Officer (ISSO). Any suspected cybersecurity incident, such as spillage of classified information to an unclassified system, regardless of the location of the computer system, must be reported immediately to the COR/TR/PM, Security's COR, ISSO, the Contractor's Facility Security Officer (FSO), and the Contracting Officer. Contractors who willfully misuse Government computer resources will be held liable to reimburse the Government for all associated costs.

IV. VISITOR CONTROL PROCEDURES.

Title 18 USC 701 provides for criminal sanctions including fine or imprisonment for anyone in possession of a badge who is not entitled to have possession. Sec.701. Official badges, identification cards, other insignia. Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both.

- a. Contractor personnel assigned to SSC Pacific will be considered long-term visitors for the purpose of this contract.
- b. Contractors that have been awarded a classified contract must submit visit requests using "only" the Joint Personnel Adjudication System (JPAS). All government activities have been directed to use JPAS when transmitting or receiving VALs. Therefore, contractors who work on classified contracts are required to have established an account through JPAS for their facility. This database contains all U.S. citizens who have received a clearance of Confidential, Secret, and/or Top Secret. The visit request can be submitted for one year. When submitting visit requests to SSC Pacific use its Security Management Office (SMO) number (660015). This information is provided in accordance with guidance provided to contractors via the Defense Security Service (DSS) website <https://www.dss.mil> (DSS guidance dated 24 April 2007, subject: *Procedures Governing the Use of JPAS by Cleared Contractors*).
- c. For visitors to receive a SSC Pacific badge their Government point of contact must approve their visit request and the visitor must present government issued photo identification.
- d. Visit requests for long-term visitors must be received at least one week prior to the expected arrival of the visitor to ensure necessary processing of the request.
- e. Code 83320 will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible SSC Pacific COR will request issuance of photo badges to contractor personnel. Identification badges are the property of the U.S. Government, will be worn in plain sight, and used for

official business only. Unauthorized use of an SSC Pacific badge will be reported to the DSS. For additional information see paragraph g below.

f. Prior to the termination of a Contractor employee with a SSC Pacific badge or active VAL on file the FSO must:

1. Notify in writing Code 83320, the COR, Security's COR, and the laboratory managers of any laboratories into which the employee had been granted unescorted access of the termination and effective date. In emergencies, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.
2. Immediately confiscate any SSC Pacific issued identification badge, vehicle decal, common access card (CAC), and return them to Code 83320 no later than five working days after the effective date of the termination.

g. Common Access Card (CAC).

1. VAL must be on file, form completed and signed, approved by the contractor's COR, and sent to the Badge and Pass Office, Code 83320.
2. All contractors coming aboard SSC Pacific will need a SSC Pacific badge whether it is a Picture or Temporary Badge. You will also need one of the following: a) Common Access Card (CAC), or 2) a Navy Commercial Access Credentialing System (NCACS). If you do not have either one of these you will need to be vetted by filling out the SECNAV 5512 which will be forwarded to NBPL for approval. Contractors will not be able to use their Retired or Dependent Military ID in lieu of the CAC or NCACS.

V. INSPECTIONS. Code 83310 personnel may conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel will cooperate with Code 83310 representatives during these inspections. A report of the inspection will be forwarded to the Contractor's employing facility and COR. The Contractor must be responsive to the Code 83310 representative's findings.

VI. REPORTS. As required by the NISPOM, Chapter 1, Section 3, contractors are required to report certain events that have an impact on the status of the facility clearance (PCL), the status of an employee's personnel clearance (PCL), the proper safeguarding of classified information, or an indication classified information has been lost or compromised.

a. The Contractor will ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 83310. If further investigation is warranted it will be conducted by Code 83310. This reporting will include the following:

1. The denial, suspension, or revocation of security clearance of any assigned personnel;
2. Any adverse information on an assigned employee's continued suitability for continued access to classified access;
3. Any instance of loss or compromise, or suspected loss or compromise, of classified information;
4. Actual, probable or possible espionage, sabotage, or subversive information; or
5. Any other circumstances of a security nature that would affect the contractor's operation on board SSC Pacific.

b. In addition to the NISPOM reporting requirements, any conviction and/or violation of the Foreign Corrupt Practices Act, or any other violation of the International Traffic in Arms Regulations (ITAR) shall immediately be reported to the Designated Disclosure Authority (DDA), COR/TR/PM and Contracting Officer.

VII. PHYSICAL SECURITY.

a. SSC Pacific will provide appropriate response to emergencies occurring onboard this command. The Contractor will comply with all emergency rules and procedures established for SSC Pacific.

- b. A roving Contract Security Guard patrol will be provided by SSC Pacific. Such coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Specific questions or concerns should be addressed to Code 83320.
- c. All personnel aboard SSC Pacific are subject to random inspections of their vehicles, personal items and of themselves. Consent to these inspections is given when personnel accept a badge permitting entrance to this command.
- d. Information about parking restrictions can be found in the SSCSDINST 5560.1F, Vehicle Parking Policy, Regulations, an Enforcement Procedures. A copy of this instruction can be obtained through your designated COR or TR.

Contractors must comply with installation access control procedures. Any Contractor who repeatedly violates access control requirements will be issued an Apparent Security Violation (ASV). After the ASV has been investigated, a letter will be forwarded to the contracting facility's Security Officer via the Center's Contracting Officer for resolution.

VIII. COR RESPONSIBILITIES.

- a. Review requests by cleared contractors for retention of classified information beyond a two-year period and advise the contractor of disposition instructions and/or submit a Final DD 254 to Security's COR.
- b. In conjunction with the appropriate transportation element, coordinates a suitable method of shipment for classified material when required.
- c. Certify and approve Registration For Scientific and Technical Information Services requests (DD 1540) (DTIC).
- d. Ensure timely notice of contract award is given to host commands when contractor performance is required at other locations.
- e. Certify need-to-know on visit requests and conference registration forms.

IX. SPECIAL CONSIDERATIONS FOR ON-SITE CLEARED FACILITIES.

Any cleared contractor facility on board SSC Pacific will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional SSC Pacific contracts may be performed in this cleared facility, but only on a case-by-case basis. The COR, Security's COR, and Contracting Officer must all be in agreement that this particular arrangement best suits the needs of the Government. At the end of this contract the on-site facility must be vacated, with proper written notification being submitted to the DSS and Security's COR.

X. ITEMS PROHIBITED ABOARD SSC PACIFIC.

The following items are prohibited within any SSC Pacific controlled areas, with the exception of personnel authorized to possess weapons in the performance of required duties.

If an individual is attempting entry onto SSC Pacific controlled spaces and discloses the possession of a weapon prior to being instructed to comply with an administrative weapons inspection, the gate guard or inspection team will deny base entry to that individual and will report the circumstances to the SSC Pacific Security Officer. If the disclosure of a firearm, explosive or dangerous weapon is made during the inspection or if no disclosure is made at all, the individual will be detained and the SUBASE Precinct will be notified.

WEAPONS

- a. Ammunition.
- b. Fireworks.
- c. Molotov Cocktail.
- d. Pipe Bomb.
- e. Black Jack.
- f. Slingshots.

- g. Billy/Sand Club.
- h. Nunchakus.
- i. Sand Bag: Partially filled with sand and swung like a mace.
- j. Metal (Brass) Knuckle.
- k. Dirk or Dagger.
- l. Switch Blade or Butterfly Knife.
- m. Knife with a blade (cutting edge) longer than 4 inches. NOTE: this represents a change from the previous 2.5-inch limit.
- n. Razor with Unguarded blade.
- o. Pipe, Bar or Mallet to be used as a club.
- p. Compressed Air or Spring Fired Pellet/BB gun.
- q. Tear Gas/Pepper Spray Weapon.
- r. Pistol, Revolver, Rifle, Shotgun or any other Firearm.
- s. Bows, Crossbows, or Arrows.
- t. Bowie Style Hunting Knife.
- u. Any weapon prohibited by State law.
- v. Any object similar to the aforementioned items.
- w. Any offensive or defensive weapons not described above, but likely to cause injury (i.e., Stun Gun, Blow Gun).
- x. Any abrasive, caustic, acid, chemical agent, or similar substance, with which to inflict property damage or personal injury.
- y. Combination Tools with Knife Blades Longer Than 4 inches (i.e., Gerber, Leatherman, etc.).

Military personnel aboard SSC Pacific controlled areas not authorized to possess a firearm, as part of prescribed military duties will be apprehended if found in possession. Civilians in unauthorized possession of a firearm will be detained while civilian authorities are notified.

CONTROLLED SUBSTANCES

Unauthorized possession or use of controlled substances defined as marijuana, narcotics, hallucinogens, psychedelics, or other controlled substances included in Schedule I, II, III, IV, or V established by Section 202 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (84 Stat. 1238) is prohibited.

CONTRABAND

Contraband defined as all equipment, products and materials of any kind which are used, intended for use, or designed for use in injecting, ingesting, inhaling, or otherwise introducing into the human body, marijuana or other controlled substances, in violation of law. This includes: hypodermic syringes, needles, and other objects to inject controlled substances in the body or objects to ingest, inhale or otherwise introduce marijuana, cocaine or hashish oil into the body is prohibited.

ALCOHOL

Permission to possess and consume alcohol on-site at SSC Pacific is at the exclusive discretion of the Commanding Officer. That includes the determinations of where and when alcohol may be brought on board the Center and consumed. SSC Pacific personnel may bring unopened containers of alcohol on board the Center, if it remains in their private vehicles except where expressly authorized for an approved event.

Open containers of any alcoholic beverage unless for use at a function approved by the SSC Pacific Commanding Officer. Employees desiring to hold a function and serve alcohol, should send a memo (hard copy) to the Commanding Officer, via the appropriate division head, the Director of Security, and the Public Affairs Officer. The Public Affairs Officer will approve or disapprove the facility use request based on availability and general use policy. If facility use is approved, the Public Affairs Officer will forward the memo to the Commanding Officer for approval/disapproval. Manufacturer sealed containers of alcoholic beverage are authorized as long as the containers remain sealed while within SSC San Diego controlled spaces. Further information is available at <https://blog.spawar.navy.mil/pacsecurity/security-info/physical-security.html>.

COUNTERFEIT CURRENCY

Counterfeit currency defined as any copy, photo, or other likeness of any U.S. currency, either past or present, not authorized by the U.S. Treasury Department is prohibited.

XI. ESCORTING POLICY.

- a. All personnel within SSC Pacific fenced perimeters, with the exception of emergency personnel such as fire, ambulance, or hazardous material response personnel responding to an actual emergency, must wear an SSC Pacific issued badge. Code 83300 or Code 83500 employees with badges displaying the word "Security" or "Safety" authorize the bearer to escort unbadged emergency vehicles and operators and support personnel during emergencies. U.S. citizens, Permanent Residents (former immigrant aliens), and Foreign Nationals may be escorted under this policy. ALL FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE SSC PACIFIC FOREIGN VISITS COORDINATOR OFFICE, CODE 83310, 553-0437.

All pictured badged SSC Pacific and co-located/tenant command employees, as well as those contractors and other government employees who have an "E" on their picture badge may escort visitors wearing a red escort-required badge

XII. CELLULAR PHONE USAGE.

- a. Cellular phone use is prohibited in all secure spaces, i.e. Open Storage areas, classified laboratories.
- b. Vehicle operators on DoD installations and operators of Government vehicles shall not use cellular phones, unless the vehicle is safely parked or unless they are using a hands-free device, and are also prohibited from wearing of any other portable headphones, earphones, or other listening devices while operating a motor vehicle.
- c. The use of cellular phones, portable headphones, earphones, or other listening devices while jogging, walking bicycling, or skating on roads and streets on Navy installations is prohibited except for use on designated bicycle and running paths and sidewalks.

XIII. PERSONAL ELECTRONIC MEDIA

- a. The use of personal electronic media (computer laptops, flash (thumb), or other removable drives) is prohibited in SSC Pacific spaces. Contact the Command Information System Security Manager (SPSC_SSCFAC_ISSM@NAVY.MIL) if you have question. All removable electronic media must be labeled (unclassified, etc.) to the highest classification of data stored, and/or for the classification of the system in which it is used. If classified, any removable electronic media must be tracked and stored appropriate to that level of classification.

CONTRACTOR REQUIREMENTS FOR ACCESS TO INTELLIGENCE INFORMATION

1. Intelligence material and information, either furnished by the user agency or generated under the contract performance, will not be:
 - a. Reproduced without prior approval of the originator of the material. All intelligence material shall bear a prohibition against reproduction while in your custody; or
 - b. Released to foreign nationals or immigrant aliens who you may employ, regardless of their security clearance or access authorization, except with the specific permission of ONI-5, via Security's COR; or
 - c. Released to any activity or person of the contractor's organization not directly engaged in providing services under the contract or to another contractor (including subcontractors), government agency, private individual, or organization without prior approval of the originator of the material, and prior approval and certification of need-to-know by the designated project manager/contract sponsor.
2. Intelligence material does not become the property of the contractor and may be withdrawn at any time. Upon expiration of the contract, all intelligence released and any material using data from the intelligence must be returned to the Contracting Officer's Representative (COR) or authorized representative for final disposition. The contractor shall maintain such records as will permit them to furnish, on demand, the names of individuals who have access to intelligence material in their custody.
3. Access to intelligence data will only be through cognizant government program managers/project engineers. Independent access is not inferred or intended.
4. Classified intelligence, even though it bears no control markings, will not be released in any form to foreign nationals or immigrant aliens (including U.S. government employed, utilized or integrated foreign nationals and immigrant aliens) without permission of the originator.
5. You will maintain records which will permit you to furnish, on demand, the names of individuals who have access to intelligence material in your custody.
6. Access to SCI intelligence data requires the adherence to the requirements set forth in the DoD 5105.21 Volumes 1 through 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security.

FOR OFFICIAL USE ONLY (FOUO) INFORMATION

1. The For Official Use Only (FOUO) marking is assigned to information at the time of its creation. It isn't authorized as a substitute for a security classification marking but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).

2. Use of FOUO markings doesn't mean that the information can't be released to the public, only that it must be reviewed by Space and Naval Warfare Systems Center Pacific, San Diego, CA prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

3. An UNCLASSIFIED document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the bottom face and interior pages.

4. Classified documents containing FOUO do not require any markings on the face of the document; however, the interior pages containing only FOUO information shall be marked top and bottom center with "FOR OFFICIAL USE ONLY." Mark only unclassified portions containing FOUO with "(FOUO)" immediately before the portion.

5. Any FOUO information released to you by Space and Naval Warfare Systems Center Pacific, San Diego, CA is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA.
EXEMPTION(S) _____ APPLY.

6. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. DO NOT REMOVE ANY FOUO MARKING WITHOUT WRITTEN AUTHORIZATION FROM SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC, SAN DIEGO, CA OR THE AUTHOR. When the FOUO status is terminated you will be notified.

7. You may disseminate FOUO information to your employees and subcontractors who have a need for the information in connection with this contract.

8. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items.

9. FOUO information may be transmitted via first-class mail, parcel post, fourth-class mail for bulk shipments only.

10. When no longer needed, FOUO information may be disposed by tearing each copy into little pieces to preclude anyone from reconstructing the document, and placing it in a regular trash, or recycle, container or in the uncontrolled burn. To ensure the document is precluded from being reconstructed it is recommended that FOUO be shredded using a crosscut shredder.

11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

12. Electronic transmission of FOUO information (voice, data, or facsimile) should be by approved secure communications systems whenever practical.

13. To obtain for official use only (FOUO) guidance refer to the DoD Information Security Program Regulation, DoDM 5200.01 Volume 4, Enclosure 3, located at http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf.

OPERATIONS SECURITY REQUIREMENTS

All work is to be performed in accordance with DoD and Navy Operations Security (OPSEC) requirements, per the following applicable documents:

- National Security Decision Directive 298
- DOD 5205.02
- OPNAVINST 3432.1
- SPAWARINST 3432.1
- National Operations Security Program (NSDD) 298
- DOD Operations Security (OPSEC) Program
- DON Operations Security
- Operations Security Policy

The contractor will accomplish the following minimum requirements in support of Space and Naval Warfare Systems Center Pacific (SSC Pacific) Operations Security (OPSEC) Program:

- The contractor will practice OPSEC and implement OPSEC countermeasures to protect DOD Critical Information. Items of Critical Information are those facts, which individually, or in the aggregate, reveal sensitive details about SSC Pacific or the contractor's security or operations related to the support or performance of this SOW, and thus require a level of protection from adversarial collection or exploitation not normally afforded to unclassified information.
- Contractor must protect Critical Information and other sensitive unclassified information and activities, especially those activities or information which could compromise classified information or operations, or degrade the planning and execution of military operations performed or supported by the contractor in support of the mission. Protection of Critical Information will include the adherence to and execution of countermeasures which the contractor is notified by or provided by SSC Pacific, for Critical Information on or related to the SOW.
- Sensitive unclassified information is that information marked FOR OFFICIAL USE ONLY (or FOUO), Privacy Act of 1974, COMPANY PROPRIETARY, and also information as identified by SSC Pacific or the SSC Pacific Security COR.
- SSC San Diego has identified the following items as Critical Information that may be related to this SOW:
 - Known or probable vulnerabilities to any U.S. system and their direct support systems.
 - Details of capabilities or limitations of any U.S. system that reveal or could reveal known or probable vulnerabilities of any U.S. system and their direct support systems.
 - Details of information about military operations, missions and exercises.
 - Details of U.S. systems supporting combat operations (numbers of systems deployed, deployment timelines, locations, effectiveness, unique capabilities, etc.).
 - Operational characteristics for new or modified weapon systems (Probability of Kill (Pk), Countermeasures, Survivability, etc.).
 - Required performance characteristics of U.S. systems using leading edge or greater technology (new, modified or existing).
 - Telemetered or data-linked data or information from which operational characteristics can be inferred or derived.
 - Test or evaluation information pertaining to schedules of events during which Critical Information might be captured. (advance greater than 3 days).
 - Details of SPAWAR/SSC Pacific unique Test or Evaluation capabilities (disclosure of unique capabilities).
 - Existence and/or details of intrusions into or attacks against DoD Networks or Information Systems, including, but not limited to, tactics, techniques and procedures used, network vulnerabilities exploited, and data targeted for exploitation.
 - Network User ID's and Passwords.
 - Counter-IED capabilities and characteristics, including success or failure rates, damage assessments, advancements to existing or new capabilities.
 - Vulnerabilities in Command processes, disclosure of which could allow someone to circumvent security, financial, personnel safety, or operations procedures.
 - Force Protection specific capabilities or response protocols (timelines/equipment/numbers of personnel/training received/etc.).
 - Command leadership and VIP agendas, reservations, plans/routes etc.
 - Detailed facility maps or installation overhead photography (photo with annotation of Command areas or greater resolution than commercially available).

- Details of COOP, SPAWAR/SSC Pacific emergency evacuation procedures, or emergency recall procedures.
 - Government personnel information that would reveal force structure and readiness (such as recall rosters or deployment lists).
 - Compilations of information that directly disclose Command Critical Information.
- The above Critical Information and any that the contractor develops, regardless if in electronic or hardcopy form, must be protected by a minimum of the following countermeasures:
 - All emails containing Critical Information must be DoD Public Key Infrastructure (PKI) signed and PKI encrypted when sent.
 - Critical Information may not be sent via unclassified fax.
 - Critical Information may not be discussed via non-secure phones.
 - Critical Information may not be provided to individuals that do not have a need to know it in order to complete their assigned duties.
 - Critical Information may not be disposed of in recycle bins or trash containers.
 - Critical Information may not be left unattended in uncontrolled areas.
 - Critical Information in general should be treated with the same care as FOUO or proprietary information.
 - Critical Information must be destroyed in the same manner as FOUO.
 - Critical Information must be destroyed at contract termination or returned to the government at the government's discretion.
 - The contractor shall document items of Critical Information that are applicable to contractor operations involving information on or related to the SOW. Such determinations of Critical Information will be completed using the DoD OPSEC 5 step process as described in National Security Decision Directive (NSDD) 298, "National Operations Security Program".
 - OPSEC training must be included as part of the contractors ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the NISPOM. NSDD 298, DoD 6205.02, "DOD Operations Security (OPSEC) Program", and OPNAVINST 3432.1, "Operations Security" should be used to assist in creation or management of training curriculum.
 - If the contractor cannot resolve an issue concerning OPSEC they will contact the SSC Pacific Security COR (who will consult with the SPAWAR/SSC Pacific OPSEC Manager).
 - All above requirements MUST be passed to all Sub-contractors.



N66001-15-R-0037 – Engineering and Support Services for Network
and Information Systems Technology Programs
Proposal No. 14.0039

SMALL BUSINESS SUBCONTRACTING PLAN

Pages 2 through 5 redacted for the following reasons:

(b)(4)